

VERBATIM**RECORD OF TRIAL²**

(and accompanying papers)

of

MANNING, Bradley E.

(Name: Last, First, Middle Initial)

PFC/E-3

(Rank)

Headquarters and

Headquarters Company,

United States Army Garrison

(Unit/Command Name)

U.S. Army

(Branch of Service)

Fort Myer, VA 22211

(Station or Ship)

By

GENERAL**COURT-MARTIAL**

Convened by

Commander

(Title of Convening Authority)

UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON

(Unit/Command of Convening Authority)

Tried at

Fort Meade, MD

(Place or Places of Trial)

on

see below

(Date or Dates of Trial)

Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012,
 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012,
 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012,
 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013,
 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013,
 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013,
 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013,
 16 August 2013, and 19-21 August 2013.

¹ Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)² See inside back cover for instructions as to preparation and arrangement.

6. Dates of Activity

From (Month/Year): 08/1988 To (Month/Year): 09/2005

Type of Employment

- Active military duty stations: { }
- National Guard/Reserve: { }
- U.S.P.H.S. Commissioned Corps: { }
- Other Federal employment: { }
- State Government (Non-Federal employment): { }
- Self-employment: { }
- Unemployment: { x }
- Federal Contractor: { }
- Other: { }

List the name of the person who can verify your unemployment.

Verifier Name: Susan Fox

Verifier's Street Address

Street: 31 Nubian Ave
City: Haverford State: MD Country: Zip Code: 20854

Verifier's Telephone Number

Number: (301) 668-5610

(End of List)

Section 12: People Who Know You Well

List three people who know you well and live in the United States. They should be good friends, peers, colleagues, college roommates, etc., whose combined association with you covers as well as possible the last 7 years. Do not list your spouse, former spouses, or other relatives, and try not to list anyone who is listed elsewhere on this form.

1. Dates Known

From (Month/Year): 01/1996 To (Month/Year): Present

Name: Thomas Paden Radford

Home or Work Address

Street: Trailer 28 4701 East Coffee Creek Road
City: Edmond State: OK Country: Zip Code: 73034

Telephone Number

Number: (405) 744-6384 Time: Night

2. Dates Known

From (Month/Year): 09/1993 To (Month/Year): Present

Name: Mark Allen Radford

Home or Work Address

Street: 18 Lakeview Drive
City: Crescent State: OK Country: Zip Code: 73028

Telephone Number

Number: (405) 280-7434 Time: Night

3. Dates Known

From (Month/Year): 08/1993 To (Month/Year): Present

Name: Jordan Scott Davis

Home or Work Address

Street: Trail 28 4701 Coffee Creek Road
City: Edmond State: OK Country: Zip Code: 73034

Telephone Number

Number: (918) 946-5121 Time: Night

(End of List)

Section 13/15: Your Spouse

Mark one item to show your current marital status.

Marital Status

- Never Married: { }
Married: { }
Separated: { }
Legally Separated: { }
Divorced: { }
Widowed: { }
Other: { }

Current Spouse (Not Applicable: { })
(No Entry Provided)

Former Spouse(s) (Not Applicable: { })
(No Entry Provided)

Section 14/15: Your Relatives and Associates

Give the full name, correct code, and other requested information for each of your relatives and associates, living or dead, specified below.

1. Mother
2. Father
3. Stepmother
4. Stepfather

-
- 5. Foster Parent
 - 6. Child (Adopted and Foster Child also)
 - 7. Stepchild
 - 8. Brother
 - 9. Sister
 - 10. Stepbrother
 - 11. Stepsister
 - 12. Half-brother
 - 13. Half-sister
 - 14. Father-in-law
 - 15. Mother-in-law
 - 16. Guardian
 - 17. Other Relative*
 - 18. Associate*
 - 19. Adult Currently Living with You

*Other Relative - include only foreign national relatives not listed in 1 - 16 with whom you or your spouse are bound by affection, obligation, or close and continuing contact. Associate - include only foreign national associates with whom you or your spouse are bound by affection, obligation, or close and continuing contact.

1. Relationship Type: Mother

Full Name
Last: Fox First: Susan Middle: Mary Suffix:

Deceased
Yes: { } No: { x }

Date of Birth
Month/Day/Year: [REDACTED]

Country of Birth
Country: UNITED KINGDOM

Country(ies) of Citizenship

1. Country: UNITED KINGDOM

(End of Country(ies) of Citizenship List)

Provide the following information if this person is living.

Current Address
Street: 31 Nubian Ave
City: Haverford West State: Country: UNITED KINGDOM

Section 15: Citizenship of Your Relatives and Associates

If your mother, father, sister, brother, child, or person with whom you have a spouse-like relationship is a U.S. citizen by other than birth, or an alien residing in the U.S., provide a Proof of Citizenship Status entry below.

Proof of Citizenship Status

-
- Provide one or more of the following to identify proof of citizenship status.

Naturalization Certificate

Certificate Number:

Provide the date issued and the location where the person was naturalized (Court, City and State).

Date Issued

Month/Day/Year: ~ / ~ / ~

Court:

Location

City: State:

Citizenship Certificate

Certificate Number:

Provide the date and location issued (City and State).

Date Issued

Month/Day/Year: ~ / ~ / ~

Location Issued

City: State:

Alien Registration

Registration Number:

Provide the date and place where the person entered the U.S. (City and State).

Date Entered U.S.

Month/Day/Year: ~ / ~ / ~

Place Entered U.S.

City: State:

Other

Provide an explanation in the space below.

Explanation

Mother is not a citizen of the United States but is a citizen of the UK.

-
- Relationship Type: Father

Full Name

Last: Manning First: Brian Middle: Edward Suffix:

Deceased

Yes: {} No: {x}

Date of Birth

Month/Day/Year: [REDACTED]

Country of Birth

Country: UNITED STATES

Country(ies) of Citizenship

1. Country: UNITED STATES

(End of Country(ies) of Citizenship List)

Current Address

Street: 3020 NW 119th Street
City: Oklahoma City State: OK Country:

Section 15: Citizenship of Your Relatives and Associates

Proof of Citizenship Status
(No Entry Provided)

3. Relationship Type: Sister

Full Name

Last: Major First: Casey Middle: Manning Suffix:

Deceased

Yes: {} No: {x}

Date of Birth

Month/Day/Year: [REDACTED]

Country of Birth

Country: UNITED STATES

Country(ies) of Citizenship

1. Country: UNITED STATES

(End of Country(ies) of Citizenship List)

Current Address

Street: 308 NW 24th ST
City: Oklahoma City State: OK Country:

Section 15: Citizenship of Your Relatives and Associates

Proof of Citizenship Status
(No Entry Provided)

(End of List)

Section 16: Your Military History

Answer the following questions.

- a. Have you served in the United States military?
Yes: {} No: {}

- b. Have you served in the United States Merchant Marine?
Yes: {} No: {}

List all of your military service below, including service in Reserve, National Guard, and U.S. Merchant Marine. If you had a break in service, each separate period should be listed. If your service was with other than the U.S. Armed Forces, identify the country for which you served.

Military History (Not Applicable: {})
(No Entry Provided)

Section 17: Your Foreign Activities

Answer the following questions.

- a. Do you have any foreign property, business connections, or financial interests?
Yes: {} No: {}

- b. Are you now or have you ever been employed by or acted as a consultant for a foreign government, firm or agency?
Yes: {} No: {}

- c. Have you ever had any contact with a foreign government, its establishments (embassies or consulates), or its representatives, whether inside or outside the U.S., other than on official U.S. Government business? (Does not include routine visa applications and border crossing contacts.)
Yes: {} No: {}

- d. In the last 7 years, have you had an active passport that was issued by a foreign government?
Yes: {} No: {}

If you answered "Yes" to one or more of the questions above, provide a detailed entry for each period of foreign activity.

(No Entry Provided)

Section 18: Foreign Countries You Have Visited

List foreign countries you have visited, except on travel under official Government orders, working back 7 years. (Travel as a

dependent or contractor must be listed.) Include short trips to Canada or Mexico. If you lived near a border and have made short (one day or less) trips to the neighboring country, you do not need to list each trip. Do not repeat travel covered in sections 9, 10, or 11.

Foreign Travels (Not Applicable: { })

1. Indicate the purpose of your visit. If you lived near a border and have made short (one day or less) trips to the neighboring country, provide the time period, purpose, country and check the "Many Short Trips" box.

Dates of Activity

From (Month/Year): 03/2006 To (Month/Year): 03/2006

Purpose of Visit

Business: { } Pleasure: { x } Education: { } Other: { }

Countries Visited

1. Country: UNITED KINGDOM

(End of Countries Visited List)

Many Short Trips: { }

2. Dates of Activity

From (Month/Year): 11/2001 To (Month/Year): 09/2005

Purpose of Visit

Business: { } Pleasure: { } Education: { } Other: { x }

Countries Visited

1. Country: UNITED KINGDOM

(End of Countries Visited List)

Many Short Trips: { }

3. Dates of Activity

From (Month/Year): 10/2004 To (Month/Year): 10/2004

Purpose of Visit

Business: { } Pleasure: { x } Education: { } Other: { }

Countries Visited

1. Country: JAPAN

(End of Countries Visited List)

Many Short Trips: { }

(End of List)

Section 19: Your Military Record

Answer the following question.

Have you ever received other than an honorable discharge from the military?

Yes: { } No: { }

If "Yes," provide the date of discharge and type of discharge below.

Date of Discharge

Month/Year: ~ / ~

Type of Discharge:

Section 20: Your Selective Service Record

Answer the following question.

a. Are you a male born after December 31, 1959?

Yes: { } No: { }

If you answered "Yes" to question a, answer the following question.

b. Have you registered with the Selective Service System?

Yes: { } No: { }

If you answered "Yes" to question b, provide your registration number. If "No," show the reason for your legal exemption.

Registration Number: 8714482562

Legal Exemption Explanation (I Do Not Know: { })

Section 21: Your Medical Record

Answer the following question.

In the last 7 years, have you consulted with a mental health professional (psychiatrist, psychologist,

counselor, etc.) or have you consulted with another health care provider about a mental health related condition?

Yes: { } No: { }

If you answered "Yes," provide an entry for each treatment to report, unless the consultation(s) involved only marital, family, or grief counseling, not related to violence by you.

(No Entry Provided)

Section 22: Your Employment Record

Answer the following question.

Has any of the following happened to you in the last 7 years?

1. Fired from a job.
2. Quit a job after being told you'd be fired.
3. Left a job by mutual agreement following allegations of misconduct.
4. Left a job by mutual agreement following allegations of unsatisfactory performance.
5. Left a job for other reasons under unfavorable circumstances.

Yes: { } No: { }

If you answered "Yes," provide a detailed entry for each occurrence to report.

(No Entry Provided)

Section 23: Your Police Record

For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

Answer the following questions.

a. Have you ever been charged with or convicted of any felony offense? (Include those under Uniform Code of Military Justice)

Yes: { } No: { }

b. Have you ever been charged with or convicted of a firearms or explosives offense?

Yes: { } No: { }

c. Are there currently any charges pending against you for any criminal offense?

Yes: { } No: { }

d. Have you ever been charged with or convicted of any offense(s) related to alcohol or drugs?

Yes: { } No: { }

31

e. In the last 7 years, have you been subject to court martial or other disciplinary proceedings under the Uniform Code of Military Justice? (Include non-judicial, Captain's mast, etc.)

Yes: { } No: { x }

f. In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s) not listed in response to a, b, c, d, or e above? (Leave out traffic fines of less than \$150 unless the violation was alcohol or drug related.)

Yes: { } No: { x }

If you answered "Yes" to a, b, c, d, e, or f above, provide an entry for each occurrence to report.

(No Entry Provided)

Section 24: Your Use of Illegal Drugs and Drug Activity

The following questions pertain to the illegal use of drugs or drug activity. You are required to answer the questions fully and truthfully, and your failure to do so could be grounds for an adverse employment decision or action against you, but neither your truthful responses nor information derived from your responses will be used as evidence against you in any subsequent criminal proceeding.

Answer the following questions.

a. Since the age of 16 or in the last 7 years, whichever is shorter, have you illegally used any controlled substance, for example, marijuana, cocaine, crack cocaine, hashish, narcotics (opium, morphine, codeine, heroin, etc.), amphetamines, depressants (barbiturates, methaqualone, tranquilizers, etc.), hallucinogenics (LSD, PCP, etc.), or prescription drugs?

Yes: { } No: { x }

b. Have you ever illegally used a controlled substance while employed as a law enforcement officer, prosecutor, or courtroom official; while possessing a security clearance; or while in a position directly and immediately affecting the public safety?

Yes: { } No: { x }

c. In the last 7 years, have you been involved in the illegal purchase, manufacture, trafficking, production, transfer, shipping, receiving, or sale of any narcotic, depressant, stimulant, hallucinogen, or cannabis for your own intended profit or that of another?

Yes: { } No: { x }

If you answered "Yes" to a or b above, provide an entry for each controlled substance or prescription drug used.

(No Entry Provided)

Section 25: Your Use of Alcohol

Answer the following question.

In the last 7 years, has your use of alcoholic beverages (such as liquor, beer, wine) resulted in any alcohol-related treatment or counseling (such as for alcohol abuse or alcoholism)?

Yes: { } No: { }

If you answered "Yes," provide an entry for each treatment to report. Do not repeat information reported in response to section 21.

(No Entry Provided)

Section 26: Your Investigations Record

Answer the following question.

a. Has the United States Government ever investigated your background and/or granted you a security clearance? If your response is "No," or you don't know or can't recall if you were investigated and cleared, check the "No" box.

Yes: { } No: { }

If you answered "Yes," provide the requested information below.

(No Entry Provided)

Answer the following question.

b. To your knowledge, have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment? (An administrative downgrade or termination of a security clearance is not a revocation.)

Yes: { } No: { }

If you answered "Yes," provide the requested information below.

(No Entry Provided)

Section 27: Your Financial Record

Answer the following questions.

a. In the last 7 years, have you filed a petition under any chapter of the bankruptcy code (to include Chapter 13)?

Yes: { } No: { }

b. In the last 7 years, have you had your wages garnished or had any property repossessed for any reason?

Yes: { } No: { }

c. In the last 7 years, have you had a lien placed against your property for failing to pay taxes or other debts?

Yes: { } No: { }

d. In the last 7 years, have you had any judgments against you that have not been paid?

Yes: { } No: { }

If you answered "Yes" to a, b, c, or d, provide an entry for each occurrence to report.

(No Entry Provided)

Section 28: Your Financial Delinquencies

Answer the following questions.

a. In the last 7 years, have you been over 180 days delinquent on any debt(s)?

Yes: { } No: { }

b. Are you currently over 90 days delinquent on any debt(s)?

Yes: { } No: { }

If you answered "Yes" to a or b, provide an entry for each occurrence to report.

(No Entry Provided)

Section 29: Public Record Civil Court Actions

Answer the following question.

In the last 7 years, have you been a party to any public record civil court actions not listed elsewhere on this form?

Yes: { } No: { }

If you answered "Yes," provide the information about each public record civil court action.

(No Entry Provided)

Section 30: Your Association Record

Answer the following questions.

a. Have you ever been an officer or a member or made a contribution to an organization dedicated to the

violent overthrow of the United States Government and which engages in illegal activities to that end, knowing that the organization engages in such activities with the specific intent to further such activities?

Yes: { } No: { }

b. Have you ever knowingly engaged in any acts or activities designed to overthrow the United States Government by force?

Yes: { } No: { }

If you answered "Yes" to a or b, explain in the space below.

Explanation

Additional Comments

Use the space below to continue answers to all other items and any information you would like to add.

Additional Comments

Certification That My Answers Are True

My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Signature (Sign in ink)

Date

(Signature on file—see Investigation Request #2665639 Signature Forms)

Expected Attachments

If you need to submit additional documents with your request, give a brief title or description of each attachment you plan to provide (e.g., map with directions to residence). Providing this list is optional; however, doing so may assist the processing offices in accounting for all attachments. Include each attachment's page count. (One sheet with content on front and back is two pages.)

Write your social security number and the Investigation Request number on the margin of each attachment you submit.

Expected Attachments
(No Entry Provided)

UNITED STATES OF AMERICA

After completing Parts 1 and 2 of this form and any attachments, you should review your answers to all questions to make sure the form is complete and accurate, and then sign and date the following certification and sign and date the release on Page 10.

Certification That My Answers Are True

My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See Section 1001 of title 18, United States Code).

Signature (Sign in ink) 	Full Name (Type or Print Legibly) Manning, Bradley E	Date Signed 20070926
Social Security Number 		



08F18704

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a security clearance.

I Understand that, for financial or lending institutions, medical institutions, hospitals, health care professionals, and other sources of information, a separate specific release will be needed, and I may be contacted for such a release at a later date. Where a separate release is requested for information relating to mental health treatment or counseling, the release will contain a list of the specific questions, relevant to the job description, which the doctor or therapist will be asked.

I Further Authorize any investigator, special agent, or other duly accredited representative of the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, the Defense Investigative Service, and any other authorized Federal agency, to request criminal record information about me from criminal justice agencies for the purpose of determining my eligibility for access to classified information and/or for assignment to, or retention in, a sensitive National Security position, in accordance with 5 U.S.C. 9101. I understand that I may request a copy of such records as may be available to me under the law.

I Authorize custodians of records and sources of information pertaining to me to release such information upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

I Understand that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 86, and that it may be redislosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for five (5) years from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner. Read, sign and date the release on the next page if you answered "Yes" to question 21.

Signature (Sign in ink)	Full Name (Type or Print Legibly)	Date Signed
	Manning, Bradley E	20070926
Other Names Used		Social Security Number 
Current Address (Street, City)	State	ZIP Code
1492 Selworthy Road Potomac	MD	20854
Home Telephone Number (Include Area Code) (301) 738-7816		

1011200717-31

31

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a security clearance.

I Understand that, for financial or lending institutions, medical institutions, hospitals, health care professionals, and other sources of information, a separate specific release will be needed, and I may be contacted for such a release at a later date. Where a separate release is requested for information relating to mental health treatment or counseling, the release will contain a list of the specific questions, relevant to the job description, which the doctor or therapist will be asked.

I Further Authorize any investigator, special agent, or other duly accredited representative of the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, the Defense Investigative Service, and any other authorized Federal agency, to request criminal record information about me from criminal justice agencies for the purpose of determining my eligibility for access to classified information and/or for assignment to, or retention in, a sensitive National Security position, in accordance with 5 U.S.C. 9101. I understand that I may request a copy of such records as may be available to me under the law.

I Authorize custodians of records and sources of information pertaining to me to release such information upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

I Understand that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 86, and that it may be rediscovered by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for five (5) years from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner. Read, sign and date the release on the next page if you answered "Yes" to question 21.

Signature (Sign in ink) 	Full Name (Type or Print Legibly) Manning, Bradley E.	Date Signed 20070926
Other Names Used		Social Security Number [REDACTED]
Current Address (Street, City) 1492 Selworthy Road Potomac	State MD	ZIP Code 20854
		Home Telephone Number (301) 738-7816

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

Instructions for Completing this Release

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position with the Federal government which requires access to classified national security information or special nuclear information or material. As part of the clearance process, I hereby authorize the Investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgement or reliability, particularly in the context of safeguarding classified national security information or special nuclear information or material?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 86 and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

Signature (Sign in ink)	Full Name (Type or Print Legibly) Manning, Bradley E	Date Signed 20070926
Other Names Used		Social Security Number [REDACTED]
Current Address (Street, City) 1492 Selworthy Road Potomac	State MD	ZIP Code 20854
		Home Telephone Number (Include Area Code) (301) 738-7816

1011200717-31

39

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

Instructions for Completing this Release

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position with the Federal government which requires access to classified national security information or special nuclear information or material. As part of the clearance process, I hereby authorize the investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgement or reliability, particularly in the context of safeguarding classified national security information or special nuclear information or material?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 86 and that it may be rediscovered by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

Signature (Sign in ink) 	Full Name (Type or Print Legibly) Manning, Bradley E	Date Signed 20070926
Other Names Used		Social Security Number 
Current Address (Street, City) 1492 Selworthy Road Potomac	State MD	ZIP Code 20854
		Home Telephone Number (Include Area Code) (301) 738-7816

40

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 10/16/07 - 10/25/07 | SID N075 | ORG ID C39 | REPORT # 01

TESTIMONIES

ITEM: 018 SOURCE: 001
NAME PERSONNEL TRAINEE DIVISION, BUILDING 470, FT.LEONARD WOOD, MO 65473
PERSONNEL RECORD
PROVIDER TOM BEREN, B-T ASSIGNMENT CLERK

ACCEPTABLE

NAME VERIFIED SSN VERIFIED DOB VERIFIED POB VERIFIED

EMPLOYMENT DATES 10/07 - 10/07
STATUS FULL TIME
WORKSIT ADDRESS CO-C- 82 BARRACKS, FT.LEONARD WOOD, MO 65473
POSITION TRAINEE
REHIRE STATUS NOT SHOWN
EMPLOYMENT STATUS CHANGE NOT APPLICABLE

ITEM: 019 SOURCE: 002
NAME BARRACKS MANAGEMENT, COMMUNITY SERVICE CENTER, BUILDING 470,
FT.LEONARD WOOD, MO 65473
RENTAL RECORD
PROVIDER JUANITA LACK, LEAD INSPECTOR
NO RECORD

TRAINEES ARE REQUIRED TO LIVE IN THE BARRACKS, NO RESIDENCE RECORDS
ARE MAINTAINED.

ITEM: 019 INVESTIGATOR'S NOTE SOURCE: 003
TRAINEES ARE REQUIRED TO LIVE IN THE BARRACKS WHILE IN BASIC TRAINING.
THIS IS ALSO THE SAME LOCATION AS THE TRAINEES EMPLOYMENT. THE
TRAINEES EMPLOYMENT RECORD LOCATION IS UNDERSTOOD TO BE THE SAME AS
THE TRAINEES RESIDENTIAL LOCATION.

ITEM: 020 SOURCE: 004
NAME MILITARY PERSONNEL DIVISION, BUILDING 470, FT.LEONARD WOOD, MO 65473
MILITARY RECORD
OBTAINED BY INVESTIGATOR

ACCEPTABLE

NAME VERIFIED SSN VERIFIED DOB VERIFIED POB VERIFIED

BRANCH OF SERVICE USA
DATE ENTERED SERVICE 10/07

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

41

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 2
DATES OF INVESTIGATION 10/16/07 - 10/25/07 | SID N075 | ORG ID C39 | REPORT # 1

DUTY STATUS ACTIVE GRADE E1

**** END OF REPORT ****

TRANSMITTED: 10/25/07 PRINTED: 01/16/08

4/2

NAME MANNING, BRADLEY | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 01/04/08 - 01/09/08 | SID Q394 | ORG ID C48 | REPORT # 01

TESTIMONIES

ITEM: 030 INVESTIGATOR'S NOTE SOURCE: 001

AUTTEMPTS TO CONTACT PADDEN RADFORD, IN PERSON, AND VIA TELEPHONE, MET WITH NEGATIVE RESULTS.

ITEM: 033 SOURCE: 002
NAME BRIAN E. MANNING, PROGRAM MANAGER, 8020 NW 119TH, OKLAHOMA CITY, OK
73162
TELEPHONE TESTIMONY

ISSUE(S) 11
PRIMARY ASSOCIATION FATHER
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT 12/17/1987 TO PRESENT

RECOMMENDS

BRIAN MANNING INDICATED HIS SON, BRADLEY MANNING, LIVED WITH HIM FROM BIRTH UNTIL 2000, EXACT DATE NOT RECALLED. BRIAN MANNING INDICATED HE AND BRADLEY'S MOTHER WERE DIVORCED AND HIS EX-WIFE WAS FROM WALES.

WHEN THEY DIVORCED, BRADLEY MANNING MOVED TO WALES WITH HIS MOTHER IN 2000, WHERE HE LIVED UNTIL 2005, EXACT DATE NOT RECALLED. BRIAN MANNING INDICATED BRADLEY MANNING LIVED WITH HIM FROM THE TIME BRADLEY MOVED BACK TO THE UNITED STATES UNTIL 04/2006, WHEN BRADLEY MOVED TO TULSA, OKLAHOMA, WHERE BRADLEY WORKED FOR INCREDIBLE PIZZA. BRIAN MANNING INDICATED BRADLEY MOVED TO MARYLAND IN 2006, EXACT DATES NOT RECALLED, TO LIVE WITH HIS AUNT, DEBORAH MANNING-VANALSTYNE. MANNING INDICATED BRADLEY ATTENDED A JUNIOR COLLEGE IN MARYLAND, EXACT NAME OF INSTITUTION NOT RECALLED. BRADLEY MANNING WAS UNEMPLOYED DURING THIS PERIOD, AS HE WAS A FULL TIME STUDENT, UNTIL HE JOINED THE MILITARY, EXACT DATE NOT RECALLED. BRIAN MANNING INDICATED HE MAINTAINS COMMUNICATIONS WITH BRADLEY, VIA TELEPHONE, EVERY TWO WEEKS ON AVERAGE.

BRIAN MANNING INDICATED BRADLEY MANNING GRADUATED FROM HIGH SCHOOL IN WALES, UNITED KINGDOM, 2005. MANNING ALSO TRAVELED TO CHINA, EXACT DATES NOT RECALLED, WITH HIS CLASS, WHILE GOING TO SCHOOL IN WALES. NO OTHER DETAILS PROVIDED.

BRADLEY MANNING IS CURRENTLY IN BOOT CAMP, EXACT LOCATION UNKNOWN.

BRADLEY MANNING GRADUATED FROM HIGH SCHOOL IN WALES, UNITED KINGDOM.

BRADLEY MANNING'S INTEREST INCLUDE MUSIC AND COMPUTERS.

BRIAN MANNING INDICATED BRADLEY MANNING DOES NOT GET ALONG WITH HIS

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

4/3

NAME MANNING, BRADLEY

| CASE # 08F18704 | PAGE 2

DATES OF INVESTIGATION 01/04/08 - 01/09/08 | SID Q394 | ORG ID C48 | REPORT # 1

STEP-MOTHER, AND THE FEELINGS ARE MUTUAL. NO OTHER DETAILS PROVIDED.

BRIAN MANNING IS NOT AWARE OF ANYTHING IN BRADLEY MANNING'S CHARACTER OR BACKGROUND WHICH COULD SERVE AS THE BASIS FOR BLACKMAIL OR COERCION.

ITEM: 033 INVESTIGATOR'S NOTE

SOURCE: 003

01/09/2008, BRIAN MANNING WAS INTERVIEWED VIA TELEPHONE, AS PER HIS REQUEST, DUE TO HIS SCHEDULE.

ITEM: 033 INVESTIGATOR'S NOTE

SOURCE: 004

BRIAN MANNING IS SUBJECT, BRADLEY MANNING'S FATHER. FATHER WAS INTERVIEWED, AS FATHER WAS LISTED VERIFIER FOR LISTED PERIOD OF UNEMPLOYMENT.

ITEM: 034

SOURCE: 005

NAME JORDAN S. DAVIS, WAL-MART ASSOCIATE, 4701 E. COFFEE CREEK ROAD, #28,
EDMOND, OK 73034

ISSUE(S) 11

PRIMARY ASSOCIATION FRIEND

AVERAGE EXTENT OF CONTACT REGULAR

SPAN OF CONTACT 1992 TO PRESENT

RECOMMENDS

JORDAN DAVIS MET BRADLEY MANNING IN KINDERGARTEN, 1992. DAVIS AND MANNING ATTENDED SCHOOL THROUGH THE EIGHTH GRADE IN CRESCENT, OKLAHOMA. DAVIS INDICATED MANNING MOVED TO WALES, UNITED KINGDOM, DUE TO HIS PARENTS DIVORCE, AND HIS MOTHER BEING FROM WALES. DAVIS MAINTAINED INFREQUENT CONTACT WITH MANNING, VIA E-MAIL, WHILE MANNING LIVED IN WALES, EXACT NUMBER OF E-MAILS NOT RECALLED. MANNING MOVED BACK TO OKLAHOMA, 11/2005, AND LIVED WITH HIS FATHER. DAVIS INDICATED FREQUENCY OF CONTACT ONE TIME PER WEEK, UNTIL MANNING MOVED TO TULSA, OKLAHOMA. DAVIS INDICATED MANNING MOVED IN WITH DAVIS FOR APPROXIMATELY THREE TO FOUR WEEKS BETWEEN LIVING WITH HIS FATHER AND MOVING TO TULSA, AND FREQUENCY OF CONTACT INCREASED TO DAILY CONTACT DURING THE PERIOD. DAVIS INDICATED HE WAS LIVING IN TULSA AT THE TIME AND MANNING LIVED WITH HIM UNTIL HE COULD FIND HIS OWN PLACE TO LIVE. MANNING AND DAVIS WORKED AT INCREDIBLE PIZZA FOR APPROXIMATELY TWO MONTHS. DAVIS INDICATED MANNING LEFT INCREDIBLE PIZZA AND TOOK A JOB WITH FYE, 06/2006. SOCIAL CONTACT CONSISTED OF EATING DINNER AND WATCHING TELEVISION, THREE TO FOUR TIMES PER WEEK. MANNING JOINED THE MILITARY 11/2007, AND CONTACT HAS BEEN LIMITED, DUE TO MANNING BEING IN BOOT CAMP.

DAVIS INDICATED MANNING LIVED IN WALES, UNITED KINGDOM, AND TRAVELED

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

144

NAME MANNING, BRADLEY

| CASE # 08F18704 | PAGE 3

DATES OF INVESTIGATION 01/04/08 - 01/09/08 | SID Q394 | ORG ID C48 | REPORT # 1

THROUGHOUT THE UNITED KINGDOM AS WELL AS EUROPE, TO INCLUDE FRANCE.
MANNING HAS ALSO TRAVELEN TO TOKYO, JAPAN.

MANNING IS CURRENTLY SERVING IN THE UNITED STATES ARMY.

MANNING'S INTEREST INCLUDE MUSIC AND COMPUTERS.

DAVIS IS NOT AWARE OF ANTHING IN MANNING'S CHARACTER OR BACKGROUND
WHICH COULD SERVE AS THE BASIS FOR BLACKMAIL OR COERCION.

**** END OF REPORT ****

TRANSMITTED: 01/09/08

PRINTED: 01/16/08

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 10/22/07 - 11/29/07 | SID T393 | ORG ID W30 | REPORT # 03

TESTIMONIES

ITEM: 002 SOURCE: 001
NAME MARY R. GIRARDI, REALTOR, 1494 SELWORTHY ROAD, POTOMAC, MD 20854
INTERVIEWED AT 7821 TUCKERMAN LANE, POTOMAC, MD 20854

ACCEPTABLE
PRIMARY ASSOCIATION NEIGHBOR
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT APPROX. 2006 TO PRESENT

RECOMMENDS

GIRARDI FIRST MET "BRADLEY" APPROXIMATELY IN 2006 WHEN THE SUBJECT MOVED INTO HIS AUNT'S HOUSE, WHICH IS LOCATED NEXT DOOR TO THE SOURCE'S HOME. THE SOURCE AND THE SUBJECT HAVE NEIGHBORLY TYPE OF CONTACT, THE SOURCE SEES THE SUBJECT ON A DAILY BASIS, AND ONCE A WEEK HAVE SMALL CONVERSATIONS WITH THE SUBJECT. THE SOURCE AND THE SUBJECT HAVE HAD NO SOCIAL CONTACT WITH EACH OTHER. THERE HAVE BEEN NO BREAKS IN THE CONTACT BETWEEN THE SOURCE AND THE SUBJECT.

THE SUBJECT RESIDES AT 1494 SELWORTHY ROAD IN POTOMAC, MARYLAND. THE SUBJECT ATTENDED MONTGOMERY COLLEGE, AND DID NOT GRADUATE FROM THERE. THE SUBJECT WAS EMPLOYED AT ABERCROMBIE AND FITCH (DISCREPANT) AND STARBUCKS . THE SUBJECT MAY HAVE JOINED THE ARMY. THE SOURCE THINKS THAT THE SUBJECT ENJOYS WORKING ON COMPUTERS AND LISTENING TO MUSIC IN HIS FREE TIME. THE SOURCE HAS NO KNOWLEDGE OF THE SUBJECT'S FOREIGN TRAVEL ACTIVITIES. THERE IS NOTHING IN THE SUBJECT'S BACKGROUND THAT WOULD LEAVE HIM SUSCEPTIBLE TO BLACKMAIL OR COERCION.

ITEM: 002 SOURCE: 002
NAME CALVIN MELONEY, GENERAL CONTRACTOR/ HOME IMPROVEMENTS, 1490 SELWORTHY ROAD, POTOMAC, MD 20854

ACCEPTABLE
PRIMARY ASSOCIATION NEIGHBOR
AVERAGE EXTENT OF CONTACT MODERATE
SPAN OF CONTACT SPRING OF 2006 TO OCTOBER 2007

DOES NOT KNOW WELL ENOUGH TO RECOMMEND

MELONEY FIRST MET "BRADLEY" IN APPROXIMATELY THE SPRING OF 2006 WHEN THE SUBJECT MOVED INTO THE HOUSE NEXT DOOR TO THE SOURCE'S HOME. THE SUBJECT IS THE NEPHEW OF THE SOURCE'S NEXT DOOR NEIGHBOR. THE SOURCE AND THE SUBJECT HAVE HAD NEIGHBORLY TYPE OF CONTACT, SAYING HELLO TO EACH OTHER IN PASSING. THE SOURCE SAW THE SUBJECT ON A DAILY BASIS, BUT REALLY ONLY HAD CONVERSATIONS WITH THE SUBJECT ON AVERAGE ONCE A

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

4/6

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 2

DATES OF INVESTIGATION 10/22/07 - 11/29/07 | SID T393 | ORG ID W30 | REPORT # 3

MONTH. THE SUBJECT ASKED THE SOURCE FOR HELP WHEN HIS ELDERLY RELATIVE FELL IN THE HOUSE AND THE SUBJECT COULD NOT LIFT HIM UP. THIS EVENT HAPPENED IN SEPTEMBER OF 2007. THE SOURCE AND THE SUBJECT HAVE HAD NO SOCIAL CONTACT WITH EACH OTHER. THERE HAS BEEN BREAKS IN THE CONTACT BETWEEN THE SOURCE AND THE SUBJECT. THE LAST CONTACT THE SOURCE HAD WITH THE SUBJECT WAS AT THE END OF SEPTEMBER OR THE BEGINNING OF OCTOBER 2007.

THE SUBJECT RESIDED IN THE HOUSE NEXT DOOR(IF FACING THE SOURCE'S HOME THE HOUSE ON THE LEFT) TO THE SUBJECT'S HOME. THE SUBJECT WORKED AT STARBUCKS. THE SOURCE HAS NO KNOWLEDGE OF WHAT THE SUBJECT ENJOYED DOING IN HIS FREE TIME. THE SOURCE HAD NO KNOWLEDGE OF THE SUBJECT'S FOREIGN TRAVEL ACTIVITIES. THE SOURCE HAD NO KNOWLEDGE OF ANYTHING IN THE SUBJECT'S BACKGROUND THAT WOULD LEAVE HIM SUSCEPTIBLE TO BLACKMAIL OR COERCION.

ITEM: 005 SOURCE: 003
NAME MONTGOMERY COLLEGE, 51 MANNAKEE STREET, SV-114, ROCKVILLE, MD 20850
EDUCATION RECORD
PROVIDER ALICE SUMMERS, TRANSCRIPT EVALUATOR
SF RELEASE

ACCEPTABLE

NAME VERIFIED	SSN VERIFIED	DOB VERIFIED	POB NOT SHOWN
DATES OF ATTENDANCE		NOT SHOWN (PART TIME)	
CAMPUS LOCATION SAME AS ABOVE			
MAJOR(S) SCIENCE-PHYSICS			
DEGREE(S) AWARDED & DATE NOT APPLICABLE			

THE ONLY DATE INDICATED ON THE SUBJECT'S TRANSCRIPT WAS SPRING 2007.

ITEM: 005 SOURCE: 004
NAME MONTGOMERY COLLEGE, 51 MANNAKEE STREET, MT 6TH FLOOR, ROCKVILLE, MD 20850
DISCIPLINARY RECORD
PROVIDER MARLENE PHILLIPS, SR. ADMIN. AIDE
SF RELEASE.

NO RECORD

ITEM: 005 INVESTIGATOR'S NOTE SOURCE: 005

THE SUBJECT WAS A PART TIME STUDENT FOR THE SPRING 2007 SEMESTER AT MONTGOMERY COLLEGE IN ROCKVILLE, MARYLAND.

ITEM: 005 INVESTIGATOR'S NOTE SOURCE: 006

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, DC 20415-4000

47

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 3
DATES OF INVESTIGATION 10/22/07 - 11/29/07 | SID T393 | ORG ID W30 | REPORT # 03

THE RECORD PROVIDER INDICATED THAT THE 2007 SPRING SEMESTER FOR MONTGOMERY COLLEGE, ROCKVILLE CAMPUS, RAN FROM JANUARY 2007 TO MAY OF 2007.

ITEM: 006 INVESTIGATOR'S NOTE SOURCE: 007

NO LOCAL EMPLOYMENT RECORDS ARE MAINTAINED. THE COMPANY USES AN AUTOMATED SYSTEM FOR EMPLOYMENT VERIFICATION.

ITEM: 006 SOURCE: 008
NAME DAVID M. RUBIN, STORE MANAGER, 5438 WESTBARD AVENUE, BETHESDA, MD 20816

ACCEPTABLE
PRIMARY ASSOCIATION SUPERVISOR
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT JANUARY 2007 TO SEPTEMBER 2007

RECOMMENDS

RUBIN FIRST MET BRAD MANNING IN JANUARY 2007 WHEN THE SUBJECT APPLIED FOR A JOB AT STARBUCKS. THE SOURCE BECAME THE SUBJECT'S SUPERVISOR.

THE SOURCE AND THE SUBJECT HAD WORK RELATED CONTACT TWO TO FOUR TIMES A WEEK, AS BOTH THE SOURCE AND THE SUBJECT WORKED DIFFERENT SHIFTS, SOME OF THE SHIFTS WOULD OVERLAP AND THAT IS WHEN THE SOURCE AND THE SUBJECT HAD WORK RELATED CONTACT. THE SUBJECT WORKED AS A BARISTA AND THE SOURCE WAS THE STORE MANAGER. THE SOURCE AND THE SUBJECT HAD NO SOCIAL CONTACT OUTSIDE OF WORK. THERE WERE NO BREAKS IN THE CONTACT BETWEEN THE SOURCE AND THE SUBJECT AT STARBUCKS. THE SOURCE'S LAST CONTACT WITH THE SUBJECT WAS AT THE END OF SEPTEMBER 2007.

THE SUBJECT ATTENDED MONTGOMERY COLLEGE. THE SUBJECT WAS PREVIOUSLY EMPLOYED AT ABACROMBIE AND FITCH(DISCREPANT) AND A MUSIC STORE BEFORE STARBUCKS. THE SOURCE HAS NO KNOWLEDGE OF WHAT THE SUBJECT ENJOYS DOING IN HIS FREE TIME. THE SOURCE HAD NO KNOWLEDGE OF THE SUBJECT'S FOREIGN TRAVEL ACTIVITIES. THERE IS NOTHING IN THE SUBJECT'S BACKGROUND THAT WOULD LEAVE HIM SUSCEPTIBLE TO BLACKMAIL OR COERCION.

ITEM: 006 SOURCE: 009
NAME ZARATH O. CANALES, STORE MANAGER, 7911 TUCKERMAN LANE, POTOMAC, MD 20854

ACCEPTABLE
PRIMARY ASSOCIATION SUPERVISOR
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT JANUARY 2007 TO SEPTEMBER 2007

DOES NOT KNOW WELL ENOUGH TO RECOMMEND

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 4
DATES OF INVESTIGATION 10/22/07 - 11/29/07 | SID T393 | ORG ID W30 | REPORT # 3

CANALES FIRST MET BRADLEY OR "BRAD" IN JANUARY 2007 WHEN THE SUBJECT STARTED WORK AT STARBUCKS. THE SOURCE AND THE SUBJECT HAD DAILY WORK RELATED CONTACT. THE SOURCE AND THE SUBJECT HAD NO SOCIAL CONTACT OUTSIDE OF WORK. THERE WERE NO BREAKS IN THE CONTACT BETWEEN THE SOURCE AND THE SUBJECT. THE SUBJECT LEFT STARBUCKS AT THE END OF SEPTEMBER TO JOIN THE UNITED STATES ARMY.

THE SUBJECT ATTENDED MONTGOMERY COLLEGE BUT DID NOT GRADUATE. THE SUBJECT WAS EMPLOYED AT STARBUCKS. THE SUBJECT IS IN THE UNITED STATES ARMY. THE SUBJECT ENJOYS WORKING ON COMPUTERS AND MUSIC IN HIS FREE TIME. THE SOURCE HAD NO KNOWLEDGE OF THE SUBJECT'S FOREIGN TRAVEL ACTIVITIES. THERE IS NOTHING IN THE SUBJECT'S BACKGROUND THAT WOULD LEAVE HIM SUSCEPTIBLE TO BLACKMAIL OR COERCION.

ITEM: 022 SOURCE: 010
NAME MONTGOMERY COLLEGE, 51 MANNAKEE STREET, ROCKVILLE, MD 20850
LAW ENFORCEMENT-OTHER
PROVIDER YASIEL RODRIGUEZ, SECURITY OFFICER
SF RELEASE
NO RECORD

**** END OF REPORT ****

TRANSMITTED: 11/29/07 PRINTED: 01/16/08

4/4

NAME MANNING, BRADLEY EDWARD

| CASE # 08F18704 | PAGE 1

DATES OF INVESTIGATION 12/06/07 - 12/07/07 | SID 0414 | ORG ID C39 | REPORT # 01

TESTIMONIES

ITEM: 001 PERSONAL SUBJECT INTERVIEW SOURCE: 001
INTERVIEW CONDUCTED UNDER UNSWORN DECLARATION ON 12/06/07 RRU BARRACKS, FIRST
FLOOR MEETING ROOM, FORT LEONARD WOOD, MO 65473

ISSUE CODE(S) 11 12

SINCE HE HAD JOINED THE ARMY HE HAS BEEN DIAGNOSED WITH A NERVE DISORDER THAT PROHIBITS HIM FROM PROPERLY PHYSICALLY PERFORMING HIS DUTIES IN THE U.S. ARMY. FOR THIS REASON HE WILL BE DISCHARGED FROM THE ARMY SOON. HE HAS NOT BEEN GIVEN A DATE THAT HE WILL BE DISCHARGED. HE HAS NOT HAD ANY DISCIPLINARY PROBLEMS SINCE HE HAS BEEN IN THE ARMY. HIS PHYSICAL INABILITY TO PERFORM HIS DUTIES AS A SOLDIER IS COMMON KNOWLEDGE TO EVERYONE IN HIS UNIT AND HIS FAMILY. INFORMATION CONCERNING THIS COULD NOT BE USED AGAINST HIM AS BLACKMAIL OR COERCION.

HIS STEP-MOTHER, SUSAN KAREN MANNING, DID NOT GET ALONG WITH HIM WHILE HE LIVED WITH HER AND HIS FATHER, BRIAN MANNING AT 8020 NW 119TH STREET IN OKLAHOMA CITY, OKLAHOMA. SUSAN KAREN MANNING DID NOT LIKE HIM BECAUSE HE WAS THE SON HIS FATHER, AND HER ESTRANGED HUSBAND, BRIAN MANNING. SUSAN KAREN MANNING AND BRIAN MANNING WERE HAVING MARITAL PROBLEMS, AND SUSAN KAREN MANNING RESENTED HIM STRICTLY FOR THAT REASON. ONE DAY IN 4/06, SUSAN KAREN MANNING CALLED THE OKLAHOMA CITY POLICE DEPARTMENT, UNKNOWST TO HIM. WHEN THE OKLAHOMA CITY POLICE DEPARTMENT ARRIVED SHE ALLEGED THAT HE HAD THREATENED SUSAN KAREN MANNING. HE DOES NOT KNOW HOW SHE ALLEGED THAT HE THREATENED HER. HE WAS NOT IN THE ROOM WHEN SHE MADE THESE ALLEGATIONS TO THE POLICE. SHE REQUESTED TO THE POLICE THAT HE BE MADE TO LEAVE THE RESIDENCE PERMANENTLY. THE POLICE DID ASK HIM TO LEAVE AND HE DID NOT OBJECT. HE GATHERED HIS BELONGINGS AND LEFT TO HIS SISTER'S HOUSE. HE STAYED WITH HIS SISTER, CASEY MANNING MAJOR FOR A FEW DAYS BEFORE HE MOVED TO MARYLAND. HE DOES NOT RECALL HIS SISTER'S PHONE NUMBER. HE DID NOT MAKE ANY THREATS AGAINST SUSAN KAREN MANNING. HE DOES NOT KNOW IF ANY POLICE REPORTS WERE MADE AGAINST HIM OR NOT. HE NEVER HEARD ANYTHING FURTHER FROM THE POLICE OR ANY COURT. HE DOES NOT BELIEVE HE WAS EVER CHARGED WITH A CRIME. HE NEVER HAD ANY PROBLEMS WITH THE POLICE PRIOR TO THIS INCIDENT. HE DID NOT HAVE ANY OTHER PROBLEMS WHILE HE LIVED THERE. HIS PARENTS, HIS SISTER AND BROTHER-IN-LAW ARE AWARE OF THIS INCIDENT. INFORMATION CONCERNING HIS STEP-MOTHER'S DISLIKE OF HIM AND ACCUSATION OF THREATS COULD NOT BE USED AGAINST HIM IN ANY WAY AS BLACKMAIL OR COERCION.

HE LIVED AT 31 NUBIAN AVENUE IN HAVERFORD WEST, UNITED KINGDOM FROM 11/01 TO 9/05. HE DID NOT LIVE AT THIS RESIDENCE TO HELP WITH CITIZENSHIP REQUIREMENTS OF ANY FOREIGN COUNTRY. HE MOVED TO THIS RESIDENCE IN 11/01 BECAUSE HIS MOTHER, SUSAN FOX, MOVED THERE AFTER

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 2

DATES OF INVESTIGATION 12/06/07 - 12/07/07 | SID 0414 | ORG ID C39 | REPORT # 1

SHE DIVORCED HIS FATHER IN 2001. HE DOES NOT RECALL MORE PRECISELY WHEN SHE MOVED BACK TO THE UNITED KINGDOM. HE WAS A MINOR CHILD AT THIS TIME AND HIS MOTHER HAD CUSTODY OF HIM. HE HAS NO CONTINUED CONTACTS WITH FOREIGN NATIONALS DUE TO HIS RESIDENCE IN ENGLAND.

HIS MOTHER, SUSAN MARY FOX, WAS ORIGINALLY BORN IN THE UNITED KINGDOM ON [REDACTED] AND A CITIZEN OF THE UNITED KINGDOM. HIS MOTHER, SUSAN FOX, MET HIS FATHER, BRIAN MANNING, WHILE HE WAS STATIONED IN THE UNITED KINGDOM WITH THE U.S. NAVY. SUSAN FOX LIVED IN THE UNITED STATES FOR ABOUT TWENTY YEARS WITH HIS FATHER, ON A GREEN CARD, BUT NEVER BECAME A U.S. CITIZEN. SUSAN FOX RETURNED TO THE UNITED KINGDOM IN 11/01. SUSAN FOX HAS NOT OCCUPATION OR EMPLOYER. SUSAN FOX IS UNEMPLOYED DUE TO A DISABILITY. SUSAN FOX HAS NO AFFILIATION WITH ANY FOREIGN GOVERNMENT. HE DOES NOT HAVE ANY FURTHER ASSOCIATION WITH FOREIGN NATIONALS AS A RESULT OF HIS ASSOCIATION WITH HIS MOTHER. HE SAW HIS MOTHER ON A DAILY BASIS IN THE U.S FROM HIS BIRTH IN 1987 UNTIL 11/01. HE SAW HIS MOTHER ON A DAILY BASIS STILL AFTER THEIR MOVE TO THE UNITED KINGDOM FROM 11/01 UNTIL HE LEFT THE UNITED KINGDOM TO LIVE WITH HIS FATHER IN 9/05. SINCE 9/05 HE HAS KEPT IN TOUCH WITH HIS MOTHER, SUSAN FOX BY TELEPHONE ONCE A WEEK. HE ALSO VISITED HER ONCE FOR A WEEK IN 3/06. THIS TRIP WAS FINANCED BY HIS FATHER. HE AND HIS SISTER, CASEY MANNING MAJOR WENT THERE TO VISIT HIS MOTHER AND HELP HER WHILE SHE WAS ILL. HIS MOTHER, SUSAN FOX, STILL LIVES AT 31 NUBIAN AVENUE IN HAVERFORD WEST, UNITED KINGDOM. SUSAN FOX IS NOT AWARE THAT HE IS UNDERGOING CONSIDERATION FOR A NATIONAL SECURITY CLEARANCE. SUSAN FOX HAS NEVER SOLICITED HIM FOR ANY ACCESS TO CLASSIFIED INFORMATION. HE HAS NOT DEVELOPED ANY SYMPATHIES, PREFERENCES OR ALLIANCES FOR ANY FOREIGN COUNTRY AS RESULT OF HIS ASSOCIATION WITH HIS MOTHER.

HE ATTENDED TASKER MILWARD VC (SCHOOL) FROM 12/01 TO 6/05. HE DOES NOT HAVE ANY LASTING CONTACT WITH ANY FOREIGN NATIONALS FROM THIS SCHOOL.

HE TRAVELED TO JAPAN FOR TWO WEEKS IN 10/04. HE TOOK THIS TRIP WITH TWENTY OTHER STUDENTS AND SPONSORS FROM TASKER MILWARD VC. THIS TRIP WAS EDUCATIONAL SIGHTSEEING TRIP OF JAPAN. HE AND THE GROUP VISITED TOKYO, JAPAN. THIS TRIP WAS FINANCED BY HIS MOTHER.

DURING ANY OF HIS FOREIGN TRAVEL: TO ENGLAND FROM 11/01 TO 9/05; TO ENGLAND FOR ONE WEEK IN 3/06; AND TO JAPAN FOR TWO WEEKS IN 10/04. HE HAS NOT HAD ANY PROBLEMS TO INCLUDE: HE DID NOT HAVE ANY PROBLEMS WITH FOREIGN GOVERNMENT OFFICIALS, LAW ENFORCEMENT, OR CUSTOMS. HE DID NOT MAKE ANY LASTING CONTACT WITH ANY FOREIGN NATIONALS. HE DID NOT NOTICE ANY EVIDENCE OF ANY MONITORING BY A FOREIGN GOVERNMENT. HE DID NOT VISIT ANY EMBASSIES OR CONSULATES. HE WAS NOT DETAINED OR ARRESTED BY ANY FOREIGN LAW ENFORCEMENT. HE DID NOT COMMIT ANY ILLEGAL OR COMPROMISING BEHAVIOR WHILE IN A FOREIGN COUNTRY. HE DID NOT STRAY FROM ANY OFFICIAL TOURS OR VISIT ANY RESTRICTED AREAS. HE DID NOT HAVE HIS PASSPORT CONFISCATED OR LOST. HE DID NOT HAVE ANY

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

NAME MANNING, BRADLEY EDWARD

| CASE # 08F18704 | PAGE 3

DATES OF INVESTIGATION 12/06/07 - 12/07/07 | SID 0414 | ORG ID C39 | REPORT # 1

PROPERTY CONFISCATED. HE DID NOT HAVE ANY SEEMINGLY ACCIDENTAL MEETINGS WITH ANY FOREIGNERS. HE WAS NOT APPROACHED BY ANY FOREIGNERS TO DEVELOP A FRIENDSHIP FOR NO APPARENT REASON.

HE WAS FIRED FROM FYE IN 6/06 FOR NOT MEETING HIS SALES GOALS. (DISCREPANT) HE FAILED TO LIST THIS FIRING FROM FYE ON HIS SF 86 AS AN OVERSIGHT. HE WAS GIVEN A VERBAL WARNING, WRITTEN WARNING AND THEN FIRED FOR NOT MEETING HIS SALES EXPECTATIONS. HE COULD NOT ESTIMATE MORE PRECISE DATES THAT THESE THINGS HAPPENED. HE WAS FIRED, VERBALLY WARNING AND WRITTEN UP ALL BY RODNEY STEWART. HE DID NOT HAVE ANY OTHER PROBLEMS AT THIS EMPLOYMENT. HE DOES NOT RECALL ANYONE ELSE THAT WOULD BE AWARE OF THIS. INFORMATION CONCERNING THIS FIRING COULD NOT BE USED AGAINST HIM AS BLACKMAIL OR COERCION. HE DOES NOT THINK THAT HE WOULD BE ELIGIBLE FOR REHIRE.

HE HAD A DIFFERENCE IN PROFESSIONAL OPINION AND STYLE THAN HIS SUPERVISOR, THOMAS CAMPBELL, AT ZOTO INC. HE ULTIMATELY LEFT ZOTO FOR THIS REASON. HE AND CAMPBELL HAD DIFFERENCES IN OPINION WHEN IT CAME TO STYLES IN WRITING SOFTWARE. HE DID NOT LIKE CAMPBELL'S STYLE, BUT HE ULTIMATELY DID IT HIS WAY BECAUSE HE WAS THE BOSS AND CEO OF THE COMPANY. THIS DIFFERENCE IN STYLES DID NOT RESULT IN ANY DISCIPLINARY ACTIONS OR POOR WORK EVALUATIONS. HE AND CAMPBELL CAME TO A MUTUAL AGREEMENT THAT IT WOULD BE BEST IF HE PURSUED ANOTHER JOB. HE WAS NOT FIRED. HE LEFT ZOTO VOLUNTARILY. HE WAS NOT TOLD TO QUIT. HE DOES NOT THINK THAT HE WOULD BE ELIGIBLE FOR REHIRE DUE TO HIS DIFFERENCE IN STYLE WITH THE CEO OF THE COMPANY. THERE ARE NO HARD FEELINGS BETWEEN HIM AND CAMPBELL. ANYONE THAT WAS AT THE COMPANY AT THAT TIME (SMALL COMPANY OF 8 PEOPLE) WOULD BE AWARE OF THEIR DIFFERENCE IN STYLES AND THE REASON FOR HIS DEPARTURE. INFORMATION CONCERNING THIS COULD NOT BE USED AGAINST HIM IN ANY WAY AS BLACKMAIL OR COERCION.

ALL OF THE INFORMATION INCLUDED ON HIS SF 86 AND PROVIDED DURING HIS PERSONAL SUBJECT INTERVIEW IS TRUE AND COMPLETE WITH THE FOLLOWING EXCEPTIONS:

HIS WORK PHONE NUMBER IS (301)765-0556. (DISCREPANT) HE DOES NOT KNOW WHY HIS SF 86 DID NOT SHOW A WORK PHONE NUMBER.

SINCE HE FILLED OUT HIS SF 86 HE HAS BEEN ACTIVE DUTY ENLISTED IN THE U.S. ARMY SINCE 10/07. (DISCREPANT) SINCE 10/07, HE HAS BEEN STATIONED AT FORT LEONARD WOOD, MISSOURI FOR BASIC TRAINING. HE DOES NOT KNOW AN ADDRESS OR PHONE NUMBER OF HIS EMPLOYER AT FORT LEONARD WOOD. HE IS A PRIVATE, E01, INTELLIGENCE ANALYST. HIS SUPERVISOR IS DRILL SERGEANT ROBINSON. HE DOES NOT KNOW AN ADDRESS, PHONE NUMBER OR FIRST NAME OF DRILL SERGEANT ROBINSON. HE HAS ALSO LIVED IN THE BARRACKS AT FORT LEONARD WOOD, MISSOURI SINCE HE ARRIVED FOR BASIC TRAINING IN 10/07. (DISCREPANT) HE DOES NOT KNOW AN ADDRESS OF THE BARRACKS THAT HE HAS STAYED IN. HIS BATTLE BUDDY, PRIVATE ANDREW DUFFEY CAN VERIFY HIS CONDUCT AND ACTIVITIES SINCE HE HAS LIVED IN THE BARRACKS AT FORT LEONARD WOOD. HE DOES NOT KNOW AN ADDRESS, OR PHONE

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 4

DATES OF INVESTIGATION 12/06/07 - 12/07/07 | SID 0414 | ORG ID C39 | REPORT # 1

NUMBER FOR PRIVATE DUFFY.

HE LIVED AT 5607 71ST PLACE EAST, APARTMENT 1005, IN TULSA, OKLAHOMA FROM 4/06 TO 7/06. HE DOES NOT RECALL ANY NEIGHBORS AT THIS RESIDENCE. HE DOES NOT THINK THAT ANY NEIGHBORS WOULD RECALL HIM AT THIS RESIDENCE, BECAUSE THIS APARTMENT COMPLEX WAS VERY TRANSIENT. THE ONLY PERSON THAT HE COULD RECALL THAT VISITED HIM THERE WAS HIS FRIEND, JORDAN DAVIS. JORDAN DAVIS LIVES AT TRAILER 28, 4701 COFFEE CREEK ROAD IN EDMOND, OKLAHOMA 73034. JORDAN DAVIS CAN BE REACHED ON HIS CELL PHONE NUMBER AT (918)946-5121.

HE LIVED WITH HIS FATHER AND STEP-MOTHER AT 8020 NW 119TH STREET IN OKLAHOMA CITY, OKLAHOMA FROM 9/05 TO 4/06. HE DOES NOT RECALL ANY NEIGHBORS AT THIS RESIDENCE. HE DOES NOT KNOW IF ANY OF THE NEIGHBORS WOULD KNOW OF HIM LIVING THERE OR NOT. HE DID NOT HAVE ANY VISITORS AT THIS RESIDENCE. THE ONLY PEOPLE THAT CAN VERIFY THIS RESIDENCE ARE HIS FATHER AND STEP-MOTHER WHO STILL LIVE THERE. HIS FATHER, BRIAN MANNING CAN BE REACHED ON HIS CELL PHONE AT (405)280-6041. DAVID SCOTT DAVIS LIVES AT 5502 E 71ST PLACE EAST IN TULSA, OKLAHOMA 74136. DAVID SCOTT DAVIS CAN BE REACHED BY TELEPHONE AT (918)728-8511. HE DOES NOT KNOW ANY OTHER CONTACT INFORMATION FOR DAVID SCOTT DAVIS.

HE LIVED AT 31 NUBIAN AVENUE IN HAVERFORD WEST, UNITED KINGDOM FROM 11/01 TO 9/05. (DISCREPANT) HE DOES NOT KNOW WHY HIS SF 86 SAYS THAT HE LIVED IN HAVERFORD, UNITED KINGDOM INSTEAD OF HAVERFORD WEST, UNITED KINGDOM.

HE LIVED AT 216 E. ADAMS STREET IN CRESCENT, OKLAHOMA FROM 11/00 TO 11/01. (DISCREPANT) HE DOES NOT KNOW WHY HIS SF 86 HAS THE WRONG STARTING DATE FOR THIS RESIDENCE.

FROM 1/92 UNTIL 11/00 HE LIVED AT RT BOX 158 IN CRESCENT, OKLAHOMA 73028. (DISCREPANT) HE DOES NOT KNOW WHY THIS RESIDENCE WAS COMPLETELY LEFT OFF HIS SF 86. HE DOES NOT KNOW A MORE PRECISE ADDRESS FOR THIS RESIDENCE. HE DOES NOT KNOW IF THIS ADDRESS IS A PHYSICAL ADDRESS OR NOT.

HE ATTENDED TASKER MILWARD VC FROM 12/01 TO 6/05. (DISCREPANT) AS AN OVERSIGHT, HE ENTERED THE WRONG STARTING DATE ON HIS SF 86 FOR THIS EDUCATION.

HE DID NOT EARN A DEGREE FROM MONTGOMERY COLLEGE OF ROCKVILLE. (DISCREPANT) HE DID NOT KNOW THAT HE WAS REQUIRED TO ENTER "N/A" FOR NOT APPLICABLE FOR ANY QUESTION ON HIS SF 86 THAT DID NOT APPLY TO HIM. THEREFORE, MONTH/YEAR DEGREE AWARDED ON HIS SF 86 ALSO DOES NOT APPLY. (DISCREPANT) HE WORKED PART TIME AT STARBUCKS FROM 1/07 TO 5/07 WHILE ALSO GOING TO SCHOOL FULL TIME AT MONTGOMERY COLLEGE OF ROCKVILLE.

HE WAS UNEMPLOYED FROM 6/06 TO 1/07. HE SPENT HIS TIME LOOKING FOR A

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

NAME MANNING, BRADLEY EDWARD

|CASE # 08F18704 |PAGE 5

DATES OF INVESTIGATION 12/06/07 - 12/07/07 | SID 0414 | ORG ID C39 | REPORT # 1

JOB AND LOOKING AT COLLEGES TO ATTEND. HE ALSO SPENT HIS TIME PLAYING ON HIS COMPUTER. HE WAS SUPPORTED FINANCIALLY BY HIS AUNT, DEBORAH VAN ALSTYN. DEBORAH VAN ALSTYN CAN VERIFY HIS ACTIVITIES AND FINANCIAL SUPPORT DURING THIS PERIOD OF UNEMPLOYMENT. DEBORAH VAN ALSTYN LIVES AT 1492 SELWORTHY IN POTOMAC, MARYLAND 20854. DEBORAH VAN ALSTYN CAN BE REACHED BY TELEPHONE AT (301)738-7816.

HE WORKED AT INCREDIBLE PIZZA CO FROM 5/06 TO 7/06. (DISCREPANT) HE DOES NOT KNOW WHY HIS SF 86 SAYS THAT HE WORKED AT THIS EMPLOYMENT FROM 9/05 TO 2/06. THIS IS INCORRECT. HE DID NOT ENTER THESE DATES FOR THIS EMPLOYMENT. HE WORKED AT INCREDIBLE PIZZA CO WHILE ALSO WORKING PART TIME AT FYE FROM 5/06 TO 6/06. HE DOES NOT RECALL ANYONE OTHER THAN THE LISTED VERIFIERS FOR HIS EMPLOYMENTS AT ZOTO, FYE AND INCREDIBLE PIZZA CO.

THEREFORE HE WAS UNEMPLOYED FROM 8/06 TO 2/06. HE SPENT HIS TIME GOING TO SCHOOL FULL TIME, LOOKING FOR A JOB ONCE HE GOT OUT OF HIGH SCHOOL, AND WATCHING TELEVISION. HE WAS SUPPORTED FINANCIALLY BY HIS PARENTS. HIS FATHER, BRIAN MANNING, CAN VERIFY HIS ACTIVITIES AND FINANCIAL SUPPORT WHILE HE WAS UNEMPLOYED DURING THIS TIME. BRIAN MANNING LIVES AT 8020 NW 119TH STREET IN OKLAHOMA CITY, OKLAHOMA 73162. HIS FATHER CAN BE REACHED BY TELEPHONE AT (405)280-6041.

HE DOES NOT KNOW WHY THE QUESTION PERTAINING TO CITIZENSHIP OF HIS RELATIVES (#15) ON HIS SF 86 WAS NOT ANSWERED. NONE OF HIS RELATIVES ARE U.S. CITIZENS BY OTHER THAN BIRTH, OR ALIENS RESIDING WITHIN THE U.S. (DISCREPANT) HIS MOTHER USED TO BE AN ALIEN RESIDING IN THE U.S. UP UNTIL THEY MOVED TO THE UNITED KINGDOM IN 11/01. WHILE SHE LIVED IN THE U.S. SHE HAD A GREEN CARD. HE DOES NOT KNOW ANY FURTHER INFORMATION CONCERNING HER GREEN CARD PRIOR TO 11/01.

THE ONLY PEOPLE THAT HE SOCIALIZES WITH IN HIS SPARE TIME ARE JORDAN DAVIS (THIRD LISTED REFERENCE ON HIS SF 86), THOMAS (GOES BY PADEN) RADFORD (FIRST LISTED REFERENCE ON HIS SF 86), AND KEVIN BROKT. HE DOES NOT KNOW AN ADDRESS OR PHONE NUMBER FOR KEVIN BROKT. HIS SECOND LISTED REFERENCE ON HIS SF 86, MARK ALLEN RADFORD IS THE FATHER OF HIS FIRST LISTED REFERENCE, PADEN RADFORD. HE DOES NOT KNOW MARK RADFORD AS WELL AS PADEN RADFORD, KEVIN BROKT OR JORDAN DAVIS.

AS AN OVERSIGHT HE FORGOT TO INCLUDE HIS STEP-MOTHER, SUSAN KAREN MANNING ON HIS SF 86 UNDER THE RELATIVES SECTION. (DISCREPANT) SUSAN KAREN MANNING IS A U.S. CITIZEN. HE DOES NOT KNOW SUSAN KAREN MANNING'S DATE OF BIRTH OR COUNTRY OF BIRTH. SUSAN KAREN MANNING LIVES WITH HIS FATHER, BRIAN MANNING AT 8020 NW 119TH STREET IN OKLAHOMA CITY, OKLAHOMA 73162.

THERE IS NOTHING IN HIS BACKGROUND THAT COULD BE USED AGAINST HIM AS BLACKMAIL OR COERCION.

ITEM: 029

SOURCE: 002

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 6

DATES OF INVESTIGATION 12/06/07 - 12/07/07 | SID 0414 | ORG ID C39 | REPORT # 1

NAME ANDREW J. DUFFEY, CANNON CREW MEMBER, 101 N. Z STREET, LOMPOC, CA
93436

INTERVIEWED AT RBU BARRACKS, FIRST FLOOR MEETING ROOM, FORT LEONARD WOOD,
MO 65473

ISSUE(S) 12
PRIMARY ASSOCIATION COWORKER
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT 10/07 - PRESENT

RECOMMENDS

ANDREW DUFFEY MET BRADLEY MANNING WHEN THEY STARTED BASIC TRAINING IN THE ARMY AT FORT LEONARD WOOD, MISSOURI. DUFFEY HAS SEEN HIM ON A DAILY BASIS IN TRAINING AND IN THE BARRACKS. THIS CONTACT CONTINUES UNTIL THE PRESENT.

HE WILL BE DISCHARGED FROM THE ARMY FOR MEDICAL REASONS. DUFFEY DOES NOT KNOW WHEN HE WILL BE DISCHARGED. DUFFEY IS NOT SURE WHO KNOWS ABOUT HIS PROBABLE MEDICAL DISCHARGE FROM THE ARMY. DUFFEY DOES NOT THINK THAT THIS INFORMATION COULD BE USED AGAINST HIM IN ANY WAY AS BLACKMAIL.

HE HAS BEEN IN THE ARMY SINCE 10/07. HE HAS NOT HAD ANY DISCIPLINARY PROBLEMS WHILE HE HAS BEEN IN THE ARMY. DUFFEY HAS NO RESERVATIONS ABOUT CONTINUING TO WORK WITH HIM IN THE FUTURE.

DUFFEY IS NOT AWARE OF ANYTHING IN HIS BACKGROUND THAT COULD BE USED AGAINST HIM AS BLACKMAIL OR COERCION.

**** END OF REPORT ****

REVISED: 01/11/08

PRINTED: 01/16/08

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 10/12/07 - 10/18/07 | SID 0721 | ORG ID C48 | REPORT # 01

TESTIMONIES

ITEM: 003 INVESTIGATOR'S NOTE SOURCE: 001

DUE TO THE TRANSIENCE OF THE NEIGHBORHOOD, ALL ATTEMPTS TO OBTAIN KNOWLEDGEABLE PERSONAL SOURCES MET WITH NEGATIVE RESULTS. FOUR NEIGHBORS WERE CONTACTED AT 8016 (1ST HOUSE EAST - SAME STREETSIDES), 8100 (2ND HOUSE WEST - SAME STREETSIDES), 8017 (1ST HOUSE NORTH - DIRECTLY ACROSS STREET), AND AT 8021 (2ND HOUSE NW - ACROSS STREET) NW 119TH ST, OKLAHOMA CITY, OKLAHOMA, ALL WITH NEGATIVE RESULTS. ALL FOUR OF THE NEIGHBORS CONTACTED MOVED INTO THEIR HOMES AFTER 9/06. NONE OF THE PEOPLE CONTACTED HAVE KNOWLEDGE OF SUBJECT AND WERE UNABLE TO PROVIDE ANY INFORMATION. TWO HOUSES AT 8024 (1ST HOUSE WEST - SAME STREETSIDES) AND AT 8025 (3RD HOUSE NW - ACROSS STREET) ARE BOTH VACANT. ATTEMPTS TO CONTACT LISTED SOURCE IN TULSA, OKLAHOMA, BY TELEPHONE MET WITH NEGATIVE RESULTS. ATTEMPTS WERE MADE ON 10/12 (FRI), 10/13 (SAT), 10/14 (MON) AND ON 10/17/07 (WED), ALL WITH NO ANSWER. NO FURTHER INFORMATION IS AVAILABLE.

ITEM: 008 INVESTIGATOR'S NOTE SOURCE: 002

ATTEMPTS TO OBTAIN SUBJECT'S RECORD INFORMATION MET WITH NEGATIVE RESULTS. THE TWO PERSONNEL IN THE OFFICE PROVIDED INFORMATION THAT RECORD INFORMATION IS NOT MAINTAINED AT THE 2-PERSON OFFICE IN OKLAHOMA CITY, OKLAHOMA, AND BOTH WERE UNABLE TO PROVIDE ANY ADDITIONAL INFORMATION. THE LISTED SOURCE TRANSFERRED TO SAN FRANCISCO, CALIFORNIA IN 8/07. ATTEMPTS TO CONTACT SOURCE BY TELEPHONE MET WITH NEGATIVE RESULTS. MESSAGES WERE LEFT AT SOURCE'S TELEPHONE NUMBER ON 10/12 (FRI), 10/15 (MON), 10/16 (TUE), AND ON 10/18/07 (THU) ALL WITH NO RESPONSE. NO FURTHER INFORMATION IS AVAILABLE.

ITEM: 013 SOURCE: 003
NAME KARA M. BARRETT, DESIGNER, ZOTO, INCORPORATED, 123 SOUTH HUDSON STREET, OKLAHOMA CITY, OK 73102

ACCEPTABLE
PRIMARY ASSOCIATION COWORKER
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT 11/05 - 4/06

RECOMMENDS

BARRETT MET BRADLEY MANNING IN 11/05 (DISCREPANT), WHEN BARRETT BEGAN EMPLOYMENT AT ZOTO, INCORPORATED, OKLAHOMA CITY, OKLAHOMA, WHERE MANNING WAS EMPLOYED AS A FULL TIME PROGRAMMER /DEVELOPER. BARRETT WORKED IN THE SAME 2-PERSON OFFICE WITH MANNING AND HAD DAILY WORK CONTACT WITH MANNING FROM 11/05 - 4/06. MANNING ENDED HIS EMPLOYMENT IN 4/06 AND BARRETT HAS NOT HAD CONTACT WITH MANNING SINCE 4/06.

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, D.C. 20415-4000

56

NAME MANNING, BRADLEY EDWARD

| CASE # 08F18704

| PAGE 2

DATES OF INVESTIGATION 10/12/07 - 10/18/07 | SID 0721 | ORG ID C48 | REPORT # 1

BARRETT DID NOT HAVE SOCIAL CONTACT WITH MANNING.

SUBJECT IS A FRIENDLY, EASY GOING, AND PLEASANT PERSON TO WORK WITH. HE IS THOROUGH, DETAIL ORIENTED, AND CONSCIENTIOUS. SUBJECT IS A TEAM PLAYER AND WORKED WELL WITH SOURCE. HE IS HONEST, TRUSTWORTHY AND STRAIGHTFORWARD. SUBJECT IS POLITE, COURTEOUS, AND RESPECTFUL. HE IS EVEN TEMPERED AND SOURCE ENJOYED WORKING WITH SUBJECT. SOURCE HAS NO KNOWLEDGE OF SUBJECT'S OUTSIDE INTERESTS OR LEISURE TIME ACTIVITIES. SOURCE IS NOT AWARE OF ANYTHING IN SUBJECT'S BACKGROUND THAT COULD BE USED AGAINST SUBJECT FOR COERCION OR BLACKMAIL.

***** END OF REPORT *****

TRANSMITTED: 10/18/07

PRINTED: 01/16/08

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 10/29/07 - 11/12/07 | SID 2994 | ORG ID C39 | REPORT # 01

TESTIMONIES

ITEM: 024 SOURCE: 001
NAME PERSONNEL TRAINEE DIVISION, BUILDING 470, FT. LEONARD WOOD, MO 65473
PERSONNEL RECORD
PROVIDER TOM BERENS, B. T. ASSIGNMENT CLERK

ACCEPTABLE

NAME VERIFIED SSN NOT SHOWN DOB NOT SHOWN POB NOT SHOWN

EMPLOYMENT DATES 10/07 - PRESENT
STATUS FULL TIME
WORKSITE ADDRESS NOT SHOWN
POSITION TRAINEE PV1
EMPLOYMENT STATUS CHANGE NOT APPLICABLE

ITEM: 025 SOURCE: 002
NAME PERSONNEL TRAINEE DIVISION, BUILDING 470, FT. LEONARD WOOD, MO 65473
MILITARY RECORD
OBTAINED BY INVESTIGATOR

ACCEPTABLE

NAME VERIFIED SSN VERIFIED DOB VERIFIED POB VERIFIED

BRANCH OF SERVICE USA
DATE ENTERED SERVICE 10/07

DUTY STATUS ACTIVE GRADE PV1

ITEM: 026 SOURCE: 003
NAME BARRACKS MANAGEMENT, BUILDING 470, FT. LEONARD WOOD, MO 65473
RENTAL RECORD
PROVIDER JUANITA LACK, LEAD INSPECTOR
NO RECORD

TRAINEES ARE REQUIRED TO LIVE IN BARRACKS. NO RESIDENTIAL RECORDS ARE MAINTAINED.

ITEM: 026 INVESTIGATOR'S NOTE SOURCE: 004
TRAINEES ARE REQUIRED TO LIVE IN BARRACKS WHILE IN BASIC TRAINING.
THIS IS ALSO THE SAME LOCATION AS THE TRAINEES' EMPLOYMENT. THE TRAINEES' EMPLOYMENT RECORD LOCATION IS UNDERSTOOD TO BE THE SAME AS THE TRAINEES' RESIDENTIAL LOCATION.

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, DC 20415-4000

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 2
DATES OF INVESTIGATION 10/29/07 - 11/12/07 | SID 2994 | ORG ID C39 | REPORT # 01

**** END OF REPORT ****

TRANSMITTED: 11/12/07

PRINTED: 01/16/08

59

NAME MANNING, BRADLEY EDWARD |CASE # 08F18704 |PAGE 1
DATES OF INVESTIGATION 12/18/07 - 12/27/07 | SID 4737 | ORG ID W30 | REPORT # 01

TESTIMONIES

ITEM: 031 SOURCE: 001
NAME DEBRA V. ALSTYNE, LAWYER, 1492 SELWORTHY ROAD, POTOMAC, MD 20854

ISSUE(S) 11
PRIMARY ASSOCIATION RELATIVE
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT 12/1987 TO PRESENT

RECOMMENDS

ALSTYNE MET BRADLEY MANNING WHEN THE SUBJECT WAS BORN AS ALSTYNE IS MANNING'S AUNT. MANNING LIVED IN OKLAHOMA FROM 12/1987 TO 12/2001 WHEN HIS PARENTS DIVORCED. ALSTYNE SAW MANNING ONCE A YEAR DURING THAT PERIOD. MANNING LIVED IN ENGLAND WITH HIS MOTHER FROM 12/2001 TILL APPROXIMATELY 10/2005.

ALSTYNE HAD NO CONTACT WITH MANNING FROM 12/2001 TO APPROXIMATELY 2004 WHEN THEY ATTENDED THE SUBJECT'S SISTER'S WEDDING. MANNING COMPLETED HIGH SCHOOL IN ENGLAND IN 07/2005 AND MOVED IN WITH HIS FATHER IN OKLAHOMA IN APPROXIMATELY 10/2005. MANNING LIVED WITH HIS FATHER AND STEPMOTHER TILL APPROXIMATELY 07/2006 WHEN HE MOVED IN WITH THE SOURCE. ALSTYNE SPOKE WITH MANNING ONE TIME WHILE HE LIVED WITH HIS FATHER, BUT SAW MANNING DAILY WHILE HE LIVED WITH THE SOURCE.

MANNING LIVED WITH ALSTYNE TILL 10/2007 WHEN HE JOINED THE US ARMY. ALSTYNE SPEAKS WITH MANNING ONCE A WEEK SINCE 10/2007.

MANNING LIVED IN ENGLAND FROM 12/2001 TO APPROXIMATELY 10/2005. THE SOURCE IS UNAWARE OF ANY PROBLEMS WITH FOREIGN OFFICIALS AS A RESULT OF THIS TIME IN ENGLAND. MANNING STILL HAS CONTACT WITH HIS MOTHER AND AUNT SHARON, BOTH CITIZENS OF THE UNITED KINGDOM, EVERY 3-4 WEEKS BY TELEPHONE.

MANNING ALSO TOOK A SCHOOL TRIP TO JAPAN IN APPROXIMATELY 2004 FOR 2 WEEKS. HE HAD NO PROBLEMS AND HAS NO CONTINUING CONTACT WITH ANY FOREIGN NATIONALS FROM THIS VISIT.

MANNING WAS UNEMPLOYED WHILE LIVING WITH THE SOURCE FROM 07/2006 TO 12/2006. HE SPENT HIS TIME RESEARCHING COLLEGES AND WAS SUPPORTED FINANCIALLY BY THE SOURCE. HE WORKED FOR STARBUCKS FROM 12/2006 TO 10/2007. MANNING ALSO TOOK 3-4 CLASSES AT MONTGOMERY COLLEGE FROM 01/2007 TO 06/2007.

MANNING ENJOYS COMPUTERS, READING AND MUSIC.

ITEM: 031 INVESTIGATOR'S NOTE SOURCE: 002

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, DC 20415-4000

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 2
DATES OF INVESTIGATION 12/18/07 - 12/27/07 | SID 4737 | ORG ID W30 | REPORT # 01

SOURCE WAS INTERVIEWED DUE TO LACK OF RESIDENTIAL AND UNEMPLOYMENT COVERAGE.

ITEM: 032 SOURCE: 003
NAME KEVIN A. BROKT, BARISTA, STARBUCKS, 7911 TUCKERMAN LANE, POTOMAC, MD
20854

ACCEPTABLE
PRIMARY ASSOCIATION SUPERVISOR
AVERAGE EXTENT OF CONTACT REGULAR
SPAN OF CONTACT APPROX 02/2007 TO APPROX 09/2007

NO REASON NOT TO RECOMMEND

BROKT MET BRAD MANNING WHEN MANNING BEGAN WORKING WITH BROKT AT STARBUCKS. BROKT WAS THE SUBJECT'S TRAINER AND SUPERVISOR AND SAW MANNING 3-4 DAYS A WEEK AT WORK UNTIL MANNING LEFT IN APPROXIMATELY 09/2007. THEY ALSO LIVED IN THE SAME NEIGHBORHOOD AND SAW EACH OTHER ONCE A WEEK AND SPOKE IN THE NEIGHBORHOOD ON THOSE OCCASIONS. THERE WERE NO GAPS IN CONTACT AND BROKT HAS HAD NO CONTACT WITH MANNING SINCE APPROXIMATELY 09/2007.

MANNING LIVED WITH HIS AUNT OFF OF FALLS ROAD IN POTOMAC, MD. HE JOINED THE US ARMY IN APPROXIMATELY 09/2007. MANNING ATTENDED HIGH SCHOOL IN ENGLAND. THE SOURCE IS UNAWARE OF THE REASON FOR THE EDUCATION OUT OF THE U.S. OR ANY DETAILS REGARDING THAT TIME PERIOD.

MANNING ENJOYS MATH, SCIENCE AND MUSIC.

**** END OF REPORT ****

TRANSMITTED: 12/27/07

PRINTED: 01/16/08

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 10/16/07 - 11/28/07 | SID 6885 | ORG ID C49 | REPORT # 02

TESTIMONIES

ITEM: 004 SOURCE: 001
NAME COOPERHILL APARTMENTS, 5607 71ST PLACE E., TULSA, OK
RENTAL RECORD
PROVIDER JOLINE ABBEY, BOOKKEEPER
SF RELEASE

ISSUE(S) 03A

NAME VERIFIED SSN NOT SHOWN DOB NOT SHOWN POB NOT SHOWN
RENT DATES 04/06-07/06 RENT PAYMENT SEE ISSUES
RENTERS BRADLEY MANNING
UNIT 5607 71ST PLACE E., APARTMENT 1005, TULSA, OK

FORWARDING ADDRESS NOT SHOWN

OCCUPANT(S) SAME AS RENTERS

RECORDS INDICATE SUBJECT MOVED INTO APARTMENT ALONE ON 4/18/06 AND
SKIPPED ON 7/12/06.

4/15/06 PAID \$155
5/1/06 PAID ON TIME \$349.00
6/12/06 PAID \$349 PLUS LATE FEES \$50
7/12/06 BOOKKEEPER JOLINE ABBY DISCOVERED APARTMENT WAS EMPTY WITH
KEYS ON COUNTER. EXACT DATE OF DEPARTURE NOT KNOWN.

CURRENT AMOUNT OWED: \$1,472.51 FOR PAST RENT, CLEANING, DAMAGES, AND
TERMINATION FEE.

NO OTHER DEROGATORY INFORMATION IN FILE.

ITEM: 004 INVESTIGATOR'S NOTE SOURCE: 002

NO PERSONAL TESTIMONY POSSIBLE AS PER BOOKKEEPER JOLINE ABBY OF
COOPERHILL APARTMENTS WHO INFORMED INVESTIGATOR THAT ALL CURRENT
RESIDENCES IN THE VICINITY OF THE APARTMENT MOVED IN AFTER SUBJECT
MOVED OUT OF THE APARTMENT.

ITEM: 007 INVESTIGATOR'S NOTE SOURCE: 003

FYI DOES NOT MAINTAIN EMPLOYMENT RECORDS. ALL EMPLOYMENT RECORDS MUST
BE OBTAINED THROUGH TRANSWORLD ENTERTAINMENT. ITEM FOR TRANSWORLD
ENTERTAINMENT WAS OBTAINED AND REPORTED.

ITEM: 009 INVESTIGATOR'S NOTE SOURCE: 004

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, DC 20415-4000

62

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 2
DATES OF INVESTIGATION 10/16/07 - 11/28/07 | SID 6885 | ORG ID C49 | REPORT # 02

INVESTIGATOR WAS UNABLE TO OBTAIN EMPLOYMENT RECORD DUE TO CONFLICT OF INFORMATION.

SOURCE UNIT DIRECTOR, JERRY BARTON INFORMED INVESTIGATOR THAT RECORDS ARE NO PERSONNEL RECORDS FOR PREVIOUS EMPLOYEES AND THAT ALL RECORDS ARE KEPT AT THE CORPORATE OFFICE. BARTON PROVIDED INVESTIGATOR WITH PHONE NUMBER OF CORPORATE OFFICE.

BARTON ALSO INFORMED INVESTIGATOR THAT THERE ARE CURRENTLY NO EMPLOYEES WORKING AT INCREDIBLE PIZZA WHO WOULD HAVE WORKED WITH SUBJECT.

INVESTIGATOR MADE PHONE CONTACT WITH THE CORPORATE OFFICE, NAME OF PERSON NOT OBTAINED, INFORMED INVESTIGATOR THAT EACH STORE KEEPS THEIR OWN RECORDS.

INVESTIGATOR MADE PHONE CONTACT WITH LISTED SUPERVISOR JOHN BRAD EDWARD, KNOWN AS BRAD EDWARD. EDWARD INFORMED INVESTIGATOR THAT HE DID NOT RECALL SUBJECT DUE TO HAVING SEVERAL EMPLOYEES, BOTH PAST AND PRESENT.

ITEM: 021 SOURCE: 005
NAME TRANSWORLD ENTERTAINMENT, 38 CORPORATE CIRCLE, ALBANY, NY 12203
PERSONNEL RECORD
PROVIDER LAUREL ROSS, HR
SF RELEASE
TELEPHONE TESTIMONY

ACCEPTABLE

NAME VERIFIED SSN VERIFIED DOB NOT SHOWN POB NOT SHOWN

EMPLOYMENT DATES 05/06 - 06/06
STATUS FULL TIME
WORKSITE ADDRESS WOODLAND HILLS MALL, TULSA, OK
POSITION LEAD ASSOCIATE/MANAGEMENT
REHIRE STATUS NOT SHOWN
EMPLOYMENT STATUS CHANGE NOT SHOWN

EMPLOYMENT DATES 5/24/06 TO 6/10/06

NO OTHER INFORMATION AVAILABLE DUE TO POLICY AND PROCEDURE.

ITEM: 021 INVESTIGATOR'S NOTE SOURCE: 006
INFORMATION WAS OBTAINED BY TELEPHONE WITH INVESTIGATOR CALLED TO OBTAIN PROCEDURE POLICY FOR OBTAINING EMPLOYMENT RECORDS.

REPORT OF INVESTIGATION
PROPERTY OF U.S. OFFICE OF PERSONNEL MANAGEMENT (IS)
1900 E ST, NW, WASHINGTON, DC 20415-4000

63

NAME MANNING, BRADLEY EDWARD

| CASE # 08F18704 | PAGE 3

DATES OF INVESTIGATION 10/16/07 - 11/28/07 | SID 6885 | ORG ID C49 | REPORT # 02

**** END OF REPORT ****

TRANSMITTED: 11/28/07

PRINTED: 01/16/08

NAME MANNING, BRADLEY EDWARD | CASE # 08F18704 | PAGE 1
DATES OF INVESTIGATION 11/02/07 - 11/09/07 | SID 7296 | ORG ID A06 | REPORT # 01

TESTIMONIES

ITEM: 023 SOURCE: 001
NAME THE WORK NUMBER, STARBUCKS COFFEE COMPANY, WWW.THEWORKNUMBER.COM,
PERSONNEL RECORD
OBTAINED BY INVESTIGATOR
TELEPHONE TESTIMONY

ACCEPTABLE

NAME VERIFIED SSN VERIFIED DOB NOT SHOWN POB NOT SHOWN

EMPLOYMENT DATES 01/07 - 10/07
STATUS NOT SHOWN
WORKSITE ADDRESS NOT SHOWN
POSITION BARISTA
REHIRE STATUS NOT SHOWN
EMPLOYMENT STATUS CHANGE NOT SHOWN

ITEM: 023 INVESTIGATOR'S NOTE SOURCE: 002

RECORD INFORMATION OBTAINED FROM THE WORK NUMBER VIA THE INTERNET.

**** END OF REPORT ****

TRANSMITTED: 11/09/07 PRINTED: 01/16/08

DATE: 02/02/12

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE

***** CASE CLOSING TRANSMITTAL *****

CLOSED: 10/02/2007

CASE #: 70696500 TYPE/SERVICE: ENTNAC - PRT

EXTRA COVERAGE:

NAME: MANNING, BRADLEY EDWARD

SSN: [REDACTED] DOB: [REDACTED]1987 POSITION:

SON: A02M
COMMANDER
BALTIMORE MEPS
850 CHISHOLM AVENUE, STOP 2995
FT MEADE, MD 20755SOI: DD70
DEPARTMENT OF DEFENSE
HQ USMEPCOM
ATTN: MOP-AD
2834 GREEN BAY ROAD
NORTH CHICAGO, IL 60064

AGENCY DATA:

OPM ADJUDICATION: F - NO ISSUES - REVIEW LEVEL 1

THE ITEM INFORMATION SUMMARIZED BELOW, AND ANY REPORTS OF INVESTIGATION, INQUIRY FORMS AND/OR OTHER ATTACHMENTS WITH THIS TRANSMITTAL, COMPLETE THE INVESTIGATION REQUESTED ON THE PERSON IDENTIFIED ABOVE.

THIS CASE HAS BEEN ELECTRONICALLY TRANSMITTED TO THE AGENCY

***** ITEM INFORMATION *****

ITEM	TYPE	ITEM IDENTIFICATION/LOCATION	CM	RESULTS
***	***	***	***	***
A01	SII		L	NO RECORD
B01	FBIF		L	NO RECORD
C01	FBIIN		L	NO PERTINENT
D01	DCII		L	NO RECORD

***** END CASE CLOSING TRANSMITTAL *****

66

PRINTED: 02/02/2012
REQUESTOR ID: F07 K115

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

Certification of Investigation

CLOSED: 10/02/2007

SUBMITTING OFFICE: SON - A02M

SECURITY OFFICE: SOI - DD70

DEPARTMENT OF DEFENSE
HQ USMEPCOM
ATTN: MOP-AD
2834 GREEN BAY ROAD
NORTH CHICAGO, IL 60064-3094

NAME: MANNING, BRADLEY EDWARD

SSN: [REDACTED] DOB: [REDACTED]/1987

POSITION:

CASE TYPE: ENTNAC

OPM CASE #: 70696500

EXTRA COVERAGE:

POSITION CODE : /

SCHEDULED DATE: 09/26/2007

INVESTIGATION CONDUCTED FROM: 7

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL

DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

67

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)
)
)
)
)

Prosecution Motion

for Preliminary Ruling on
Admissibility of Evidence
(Business Records)

Enclosure 4

22 June 2012

PROSECUTION EXHIBIT 4 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE OF PAGES

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. It was the regular practice of the business activity to make the records; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

1. STUDENT PORTAL RESERVATION by STUDENT FUNCTION (TRAINING HISTORY ALL) MANNING, BRADLEY (9504).
2. IET TRAINEE PROCESSING, MANNING, BRADLEY (9504).

Organization

HQ DA G-1 (DAPE-MPT) Pentagon 3001TRNG WASH. DC. 0300 20310-

Signature

Ralph E Steinway

Date

11 JUNE 2012

Print or Type Name

RALPH E. STEINWAY

Title

C, TRNG DIVISION

Business Telephone

703 695 5914

Business Address

Same As Above

Subscribed and sworn to before a notary public, this 11 day of JUNE, 2012.

Notary Public

My commission expires on:

INDEF. PER 10 USC 1044A


[Logon & Logoff](#) • [Help Desk](#) • [FAQs](#) • [ATRRS Comments](#) • [Portal Help](#) • [ATRRS Homepage](#) • [Renew Password](#) • [Channels](#) • [Logon Assistance](#) • [Reports Generator](#)

Input Parameters: SSN

[Update Parameters](#)

Student Menu

 Student
 Portal -
 Reservations
 By Student
 Function
 (RS)
[Jump To Another Portal](#)

*** Where Applicable, Double-Click on Textbox for List of Valid Verification Table Values ***

Original SSN:	Correct SSN:	For SSN Corrections ONLY	
Name: MANNING BRADLEY E	Pay Grade: E2	Gender: MALE	DLAB: 000
Address: 1492 SELWORTHY ROAD	City: POTOMAC	State: MD	ZIP: 20854 - 0000
Duty Position:		MOS:	35F1
E-Mail: BRADLEY.MANNING@US.ARMY.MIL			
Security Clearance: M	Branch:	Functional Area:	Civilian Series:
Handicapped: <input checked="" type="radio"/> Yes <input type="radio"/> No	Career Program:	Unit ID Code: W1E88D	Rank:
Payplan: E	Grade / Pay Band: 02		
DLPT (LRS): 00 00 00	DTDLPT (YYMM):		
ASI: SQI: LIC: YY MEL: Y MES: 9			

[Sub-Courses Report](#): [Save to Excel](#), [View in Browser](#), [Text File](#)

NOTE: The Sub-Courses Report does NOT pull the entire RS Function. It only pulls AIPD Correspondence Courses for the Student.

Student Reservations

Expand All Records: Yes No

9 Total Reservations

Clear Delete:

View:

Page 1 of 1

Delete All Student Information

<input checked="" type="radio"/>	Del	Preq	FY	School	Course	Ph	Class	RS	RRC	IS	IRC	OS	ORC	QS	CP	Remark	ShipStat
<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	2012	562	SMARTFORCE		00A	R			I			6B	7EA		
<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	2011	562	SMARTFORCE		00A	R		I		G		6B	7EA		
<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	2010	562	SMARTFORCE		00A	R		I		G		6B	7EA		
<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	2009	562	SMARTFORCE		00A	R		I		G		6B	7EA		
<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	2008	562	SMARTFORCE		012	R		I		G		6B	7EA		
<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	2008	301	243-35F10		027	R		I		G		WJ	ANM		

Class Location: FT HUACHUCA, AZ 85613-6000 Course Title: INTELLIGENCE ANALYST

Ship Status:

Report Date: 2008-04-11 Start Date: 2008-04-14 End Date: 2008-08-14

Original Source: TA	Original Date: 2008-01-23	Original Logonid: REL3D
Last Source: RG	Last Date: 2008-08-14	Last Logonid: CKB05

AATAS ID:	Current Level:	Next Level Access:
Application Pointer:	Action Officer ID:	

<input type="checkbox"/>	2008	807	750-BT	015	Q	G	WJ	ANM
--------------------------	------	-----	--------	-----	---	---	----	-----

Class Location: FT LEONARD WOOD, MO 65473-5000 Course Title: BASIC COMBAT TRAINING

Ship Status:

Report Date:	2008-01-21	Start Date:	2008-01-25	End Date:	2008-04-03
--------------	------------	-------------	------------	-----------	------------

Original Source:	TA
Last Source:	HO

Original Date:	2008-01-23
Last Date:	2008-04-07

Original Logonid:	REL3D
Last Logonid:	COA01

AATAS ID:	
Application Pointer:	

Current Level:	
Action Officer ID:	

Next Level Access:	
--------------------	--

			2008	807	750-BT	002	I	L	H8	WJ	ANM
			2008	807	RECBN	011	I	G		WJ	ANM

[Update Student Info](#)

9 Total Reservations

Page 1 — of 1

For Official Use Only

The information presented on this web site can not be reused, copied, duplicated, or distributed for non-ATRRS purposes without written permission from Military Personnel Management (DAPE-MPT), HQDA Army G-1, U.S. Army. This page was generated on June 11, 2012 at 12:21:29 ET from data provided by Army Training Requirements and Resources System (ATRRS).

[Privacy and Security Notice](#)

ATRRS

Army Training Requirements and Resources System

"The Link To A Trained
And Ready Force"

Logout • Logoff • Help Desk • FAQs • ATRRS Comments • Portal Help • ATRRS Homepage • Renew Password • Channels • Logon Assistance • Reports Generator																																												
Input Parameters: MPPFLAG [P] FY 2008 SCH [001] TCRS [F43-35F10] PHASE [] CLS [007] ISSN [445989504] Update Parameters																																												
STRAMS-E Menu STRAMS-E Portal - IET Trainee Processing (TA) Jump To Another Portal																																												
TJ2 - Grad date must be > today to schedule new training																																												
Fiscal Year: 2008 School: 301 - US ARMY INTELLIGENCE COE, FT HUACHUCA, AZ Course: 243-35F10 Phase: Class: 027 Company #: F22 Report Date: 2008-04-11 Start Date: 2008-04-14 End Date: 2008-08-14 URC: W1E8D PPA: AH																																												
Name: MANNING BRADLEY E SSN: 445989504 Enrollment: <input type="button" value="ENROLL"/> Q.S.: WJ CP: ANM Component: <input type="button" value="Active"/> Res Status: R Input Status: I Output Status: G RES Reason: Input Reason: Output Reason: Graduation Date: <input type="button" value="001"/> 2008-08-14 Paygrade: <input type="button" value="E2"/> DOB: <input type="button" value="01"/> 1987-12-17 Gender: <input checked="" type="radio"/> Male <input type="radio"/> Female Height: <input type="button" value="5'2"/> Mental Status: <input type="button" value="SINGLE"/> Racial Group: <input type="button" value="CAUCASIAN"/> Citizenship: <input type="button" value="NATIVE BORN"/> PULHES: <input type="button" value="111121"/> ENTNAC Results Received? Yes PSR: <input type="button" value="A"/> Date PSR: 2007-09-26 PSIC: X Date PSIC: 2008-10-08																																												
Education and Scores <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>GT</th><th>GM</th><th>EL</th><th>CL</th><th>MM</th><th>SC</th><th>CO</th><th>FA</th><th>DF</th><th>ST</th><th>DRYBAT</th><th>MA</th><th>SC</th><th>CELC</th><th>DLAB</th><th>AAT</th> </tr> </thead> <tbody> <tr> <td>125</td><td>126</td><td>127</td><td>126</td><td>121</td><td>128</td><td>128</td><td>126</td><td>126</td><td>126</td><td>600</td><td>1</td><td>2</td><td>3</td><td>C</td><td>900</td><td>00</td> </tr> </tbody> </table>												GT	GM	EL	CL	MM	SC	CO	FA	DF	ST	DRYBAT	MA	SC	CELC	DLAB	AAT	125	126	127	126	121	128	128	126	126	126	600	1	2	3	C	900	00
GT	GM	EL	CL	MM	SC	CO	FA	DF	ST	DRYBAT	MA	SC	CELC	DLAB	AAT																													
125	126	127	126	121	128	128	126	126	126	600	1	2	3	C	900	00																												
Ultimate MOS: <input type="button" value="35F1"/> Training LIC: <input type="button" value=" "/> Enlistment Committ: <input type="button" value="UNCM"/> Previously ACO MOS: <input type="button" value=" "/> Previously ACO LIC: <input type="button" value=" "/> Enlisted ASI: <input type="button" value=" "/> Enlisted SQI: <input type="button" value=" "/> Commitment MOS: <input type="button" value="35F1"/> DLPT (LRS): <input type="button" value="00"/> <input type="button" value="00"/> <input type="button" value="00"/>																																												
ETS Date: <input type="button" value=" "/> Term Enlist: <input type="button" value="48"/> ASCO: <input type="button" value=" "/>																																												
RedGreen Visitor: <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No CONAP: <input type="button" value="W"/> <input type="button" value=" "/> <input type="button" value=" "/> <input type="button" value=" "/> Driver's License: <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No ORSAM: <input type="button" value="GM"/> <input type="button" value="KS"/> <input type="button" value=" "/> Split Training: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Warmor Status: <input type="button" value=" "/> Bonus: <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Prior Service: <input type="button" value="N"/>																																												
Hometown Recruiter (HRAP): No HRAP Start Date: <input type="button" value="00-01-01"/> HRAP End Date: <input type="button" value="00-01-01"/> Buddy Team (BTAP) Name: BTAP SSN: <input type="button" value=" "/>																																												
Recycle To Another Class: <input type="button" value="FY"/> <input type="button" value=" "/> SCH <input type="button" value=" "/> <input type="button" value=" "/> CLS <input type="button" value=" "/> Reason: <input type="button" value=" "/>																																												
End of Training Data and Assignment Data Are Automatically Determined On Update. End of Training Date: <input type="button" value="00-01-01"/> 2008-08-14 Assignment Date: <input type="button" value="00-01-01"/> 2008-08-21 Available for Assignment: <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Discharge Date: <input type="button" value="00-01-01"/> Discharge Reason: <input type="button" value=" "/> Go To Next SSN: <input type="button" value=" "/>																																												

TRANSACTION LOG INFORMATION

[Update Information](#)

For Official Use Only

The information presented on this web site can not be reused, copied, duplicated, or distributed for non-ATRRS purposes without written permission from Military Personnel Management (DAPE-MPT), HQDA Army G-1, U.S. Army. This page was generated on June 11, 2012 at 12:27:14 ET from data provided by Army Training Requirements and Resources System (ATRRS).
 Privacy and Security Notice

UNITED STATES OF AMERICA
v.
Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Motion

**for Preliminary Ruling on
Admissibility of Evidence
(Business Records)**

Enclosure 5

22 June 2012

PROSECUTION EXHIBIT 3 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE OF PAGES

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. It was the regular practice of the business activity to make the records; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

DVD-R CONTAINING TWO RTF FILES NAMED
243-35F10 Ver1 POI.rtf
243-35F10 Ver1 Lesson Plans.rtf

Organization

EDO 305th MI BN

Signature

Date

13 FEB 2012

Print or Type Name

ANTHONY L BENNETT

Title

35F10 Committee CHIEF

Business Telephone

500-538-6429

Business Address

FT MUECHICA, AZ

The attached record consists of

1 Disc pages 2 files).

Subscribed and sworn to before a notary public, this 1st day of February, 2012.

Notary Public

Rober Ginters, SGT, US Army

Commission expires:

JUDGE ADVOCATE
UNITED STATES
ARMY

Indef.



Prosecution Exhibit 5
(Attachments)
have been entered into
the record as a CD/DVD
and will be maintained
with the original
Record of Trial

UNITED STATES OF AMERICA

**Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211**

1

1

1

10

1

1

1

Prosecution Motion

**for Preliminary Ruling on
Admissibility of Evidence
(Business Records)**

Enclosure 6

22 June 2012

92

~~PROSECUTION EXHIBIT 6 for identification
PAGE OFFERED. ADMITTED.
PAGE 6 OF 6 PAGES~~

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

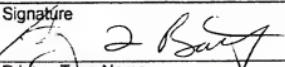
1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. It was the regular practice of the business activity to make the records; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

1. 3SF10 STUDENT EVALUATION PLAN (SEP)
2. Memo Verifying Instructors in the particular class-room
3. CLASS 3SF10-027 ROSTER

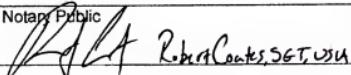
Organization

E^c 305th MI BN

Signature	Date
	6 FEB 2012
Print or Type Name	Title
Anthony L. BARNETT	CHIEF 35F COMM. TEE
Business Telephone	Business Address
520-538-6428	DAVIS HALL, Ft. WORTH, TX

The attached record consists of 17 pages (3 files).

Subscribed and sworn to before a notary public, this 6th day of February

Notary Public

Robert Coats, SGT, USA

My commission expires on:

Indefinite



**STUDENT EVALUATION PLAN (SEP)**

COURSE: 243-35F10 (V10)
COURSE TITLE: Intelligence Analyst Course
APPROVAL DATE: 01 December 2007
IMPLEMENTATION DATE: 01 December 2007
APPROVAL AUTHORITY: Commander, 305th MI Battalion
111th MI Brigade
Fort Huachuca, Arizona 85613-7002
SUPERSESSION INFO: This SEP Supersedes All Previous Versions
PROPONENT SCHOOL: US Army Intelligence Center & Fort Huachuca
Fort Huachuca, AZ 85613-7002

1. Purposes and Scope.

- a. This SEP establishes student responsibilities and course requirements for the 243-35F1O, Intelligence Analyst Course.
- b. This SEP identifies the requirements for course tests and performance standards, general standards (AR 350-1, etc.), counseling, retraining, re-testing, relief from course, academic performance ratings, grievances, and redress procedures.
- c. The purpose of this course is to train, evaluate and certify Soldiers in selected skill level one MOS related tasks.
- d. Cochise Community College, Sierra Vista, Arizona will award college semester credit hours at completion of this course. The American Council on Education (ACE) recognizes college credits earned, for the completion of this course, in degree completion programs at other colleges.
- e. This SEP is punitive. Violations of this SEP may be punished under Art 92, UCMJ as a violation of a lawful regulation.

2. Individual Course Examinations & Performance Objectives. Student evaluations are performance-based. A detailed rating explanation of the DA 1059, Academic Evaluation Report (AER) is found in Paragraph 5 of this SEP. Each academic evaluation is outlined below showing the Performance Objectives which are tested, and the minimum test standards required to pass. There are no pre-testing procedures in the 35F1O course.

Module & Lesson Plan	Instruction	Critical Task Trained	Performance Objective	Exam Standard	DA 1059 Block
Module A (Basic Skills) 35F1A02L	Information Security	1004	A. Annotate Classification Markings to Documents/Media B. Apply Procedures for Protecting Classified Information	12/15 12/15 80% standard	Item 12E
Module A 35F1A03L	Research, Writing, and Rhetoric (R3)	1104,1105,1457	A. Present Intelligence Findings	GO / NO GO 100% standard	Item 12B,E, A
Module A 35F1A04L	Map Reading and Symbology	1000, 1002, 1404, 1160	A. Perform Military Map Reading Functions B. Maintain a SiTMAP C. Maintain an Incident Overlay	19/25 6/6 5/7 74% standard	Item 12A

Module B (IPB Skills) 35F1B02L	Intelligence Preparation of the Battlefield (Step 2)	1150,1151,1152	A. Create a Modified Combined Obstacle Overlay (MCOO) for Phase III Operations B. Create a Modified Combined Obstacle Overlay (MCOO) for Phase IV Operations C. Determine Weather Effects on Operations	4/5 10/13 8/10 79% standard	Item 12A
Module B 35F1B03L	Intelligence Preparation of the Battlefield (Step 3)	1158, 1202, 1456	A. Build a Threat Model for Phase III Operations B. Build a Threat Model for Phase IV Operations	8/10 12/15 80% standard	Item 12A
Module B 35F1B04L	Intelligence Preparation of the Battlefield (Step 4)	1153, 1154, 1458	A. Determine Most Probable Threat Course of Action for Phase III Operations B. Determine Most Probable Threat Course of Action for Phase IV Operations	8/11 4/5 76% standard	Item 12A
Module C (ISR & Targeting Skills) 35F1C01L	Intelligence, Surveillance, and Reconnaissance (ISR)	1050, 1057, 1501	A. Draft an ISR Plan for Phase III Operations B. Draft an ISR Plan for Phase IV Operations	43/54 43/54 80% standard	Item 12E
Module C 35F1C02L	Targeting	1005, 1204	A. Identify Elements of the Targeting Process B. Conduct Targeting in a Phase III Operation C. Conduct Targeting in a Phase IV Operation	8/10 24/33 20/25 77% standard	Item 12E
Module D (Capstone) 35F1D01L	Automated Intelligence Systems (AIS)	1053, 1101, 1102, 1601	A. Determine best multiple choice question correctly B. Create a visual tool in Pathfinder C. Conduct Map Operations D. Display the Current Situation	3/4 GO-NO-GO 5/7 2/3	Item 12A,D
Module D	FTX	1004, 1454	A. Produce an Intelligence Summary	GO-NO-GO	Item 12A,B,C,D

35F1D02L			B. Conduct a Military Briefing C. Develop an Incident Overlay and HVT list D. Perform Collection Management Ops	GO-NO-GO GO-NO-GO GO-NO-GO 100% standard	
----------	--	--	---	---	--

3. General Standards.

a. **Standards of Conduct.** Students will conduct themselves in the manner expected of any military professional. This includes demonstrating law-abiding personal conduct and behavior, both on and off duty. The Commanding General of the US Army Intelligence School and Center, the 111th MI Bde Commander, or the 305th MI Bn Commander may relieve students from the course for any conduct or behavior that violates any local, state, or federal law (including the Uniform Code of Military Justice), or for any conduct or behavior that violates any Department of Defense (DoD), Department of the Army, or local, regulation or policy. This includes integrity (e.g. cheating/plagiarism) and fraternization issues (e.g. senior-subordinate or student-cadre). See Paragraph 3j, for more information concerning relief actions.

b. Army Physical Fitness Test (APFT)/ Weight Control.

- (1) **Body Composition standards:** IAW TRADOC Regulation 350-6, accessions standards for body composition as stated in AR 40-501, paragraph 2-21b, apply after the first year of IET Soldier's active duty service. The standards of AR 600-9, table 2, are applicable after the initial year of service. Soldier's that exceed one year of service and fail to meet the body composition standards IAW AR 600-9, table 2, will ship to gaining unit with documentation forwarded to include the flag (transferable). Military Occupational Specialty – Transition (MOS-T) Soldiers must meet the requirements of AR 600-9, table 1 IAW TRADOC Regulation 350-6 paragraph 3-4f. MOS-T with temporary profiles which prevent completion of APFT in a MOS producing course will not be enrolled. Soldiers in temporary duty (TDY) and return status that do not meet body composition standards prescribed in AR 600-9 will not attend a MOS producing course and will be returned to their home station. Soldiers in TDY en route or permanent change of station not meeting the prescribed body composition standards in AR 600-9, table 2, will not be allowed to attend a MOS producing course. These Soldiers will be attached to TRADOC subordinate commands, pending clarification of assignment instructions for follow-on training.
- (2) **Army Physical Fitness Test (APFT):** IAW TRADOC Regulation 350-6, paragraph 4-3c (3). A diagnostic APFT is administered at least once a month through the 20th week of training. Phase V+ Soldiers that have met the APFT standards for graduation will take the APFT IAW AR 350-1, paragraph 1-24. A record APFT is administered no later than the last 2 weeks of training, to determine if the Soldier has achieved the APFT standards for graduation (60 points per event; 180 minimum total points). Phase IV, V, and V+ IET Soldiers with permanent profiles will take the APFT within the limits of their profile. IAW TRADOC Regulation 350-6, paragraph 4-3c (4), MOS-T Soldiers must pass the APFT as a graduation requirement for a MOS producing school. The Soldier's Company Commander may direct any Soldier to weigh-in at any time during the course, IAW AR 600-9.
- (3) Soldiers who meet academic course requirements, but fail to meet the physical fitness and height/weight standards will not be removed from the course, nor will they be required to re-attend the course if all other course requirements are met. Instead, soldiers will complete training and their DA form 1059 will be annotated to reflect their performance.

- i) Soldiers who fail to meet the APFT standards will be considered an academic course graduate, but item 11.c of their DA form 1059 will be marked failed to achieve course standards and item 14 will be marked failed to meet APFT standards.
 - ii) Soldiers who fail to meet the body fat composition standards of AR 600-9 will be considered an academic course graduate, but item 11.c. of their DA form 1059 be marked marginally achieved course standards and item 14 will be marked failed to meet body fat composition standards.
 - iii) Soldiers who fail to meet the Army standards for both the APFT and body fat composition will be considered an academic course graduate, but item 11.c of their DA form 1059 will be marked marginally achieved course standards and item 14 will be marked failed to meet APFT standards and failed to meet body fat composition standards.
- c. Soldiers who fail to meet the APFT and weight control Standards, their DA form 1059 and graduation certificate will not be held at the institution. Previously held DA form 1059s and graduation certificates will be released to the soldier's unit IAW this message. Unit Commanders/Command Sergeants Major are expected to counsel soldiers and take appropriate actions to correct deficiencies for all soldiers failing the APFT and/or height/weight standards at institutional training. This policy does not apply to Initial Military Training Soldiers (IMT). Rules governing APFT and Weight Control requirements are contained in TRADOC Regulation 350-6.
- d. **Standards of Responsibility and Accountability.**
- (1) Students will properly maintain and secure all government issued equipment. Loss or damage to any government issued equipment may result in a Financial Liability Investigation of Property Loss. If the student is found to be at fault, the actions could result in a statement of charges, UCMJ action, and possible relief from the course.
 - (2) Students will properly maintain and secure all classified information and material. If a student fails to properly maintain or secure classified information or materials, the security violation will be reported to proper investigative command and will be handled accordingly IAW AR 380-5.
 - (3) If the student obtains a physical profile that interferes with his/her completion of the course, academically or physically, the student may be recycled, or may be medically removed from the course entirely. The student may apply for readmission to the 35F1O course at a later date.
- e. **Required Attendance.** All instruction is considered critical. Absence from any training will have a negative effect on the student's ability to achieve the training objectives. Approval to miss any portion of the course for any length of time must be coordinated and approved by the Course Manager or his/her designee. The student is responsible for obtaining notes on all missed course material. A Soldier may be considered for administrative recycle if they miss 7 consecutive or 15 cumulative academic hours. The 35F1O Course OIC will consider, on a case-by-case basis, any recycle action(s) for Soldiers who miss academic hours.
- f. **Remedial Training and Retesting.** An initial test failure will result in retraining within 24 hours and one reexamination. As an exception to policy, the 35F1O Committee OIC may, when extraordinary circumstances are present, allow a Soldier a second retest. Such extraordinary circumstances must clearly demonstrate that the Soldier's failure was through no fault of his/her own. The burden of proof falls upon the Soldier. The 35F1O Course NCOIC will coordinate the reexamination dates and schedules for all reexaminations.
- g. **Grade Adjustment Procedures:** Student grades may be adjusted on a case-by-case basis when it is found that it was no fault of the student. The Committee OIC will be the ultimate authority for grade adjustment.

h. Academic Probation.

(1) IAW Company D and Company C Standard Operating Procedures (SOP), Soldiers that fail an exam will be placed on Academic Probation until they pass the next initial examination. Soldiers who are recycled per a retest failure will remain on Academic Probation until they pass the next examination, which caused them to recycle. IAW paragraph 4c of this SEP, instructors will counsel all Soldiers who fail an exam and inform them of Academic Probation, mandatory remedial training and study hall requirements. The counseling session will outline, specifically, the appropriate actions to follow.

i. Recycle Actions. This refers to being removed from the current class and being placed in the next available class in the instruction cycle.

(1) The Battalion Commander is the approval authority for a student's initial recycle.

(2) An academic recycle will occur if a Soldier fails a retest IAW TR 350-18.

(3) An administrative recycle may occur for reasons other than academic reasons (i.e. medical, discipline, etc.)

(4) As stated earlier, a Soldier may be considered for administrative recycle if they miss 7 consecutive or 15 cumulative hours of academic time. The 35F Course OIC will consider, on a case-by-case basis, any recycle action(s) for Soldiers who miss more than 7/15 academic hours.

(5) The 35F Course OIC or designated representative will make the determination as to which phase of instruction the Soldier will be recycled into. Students are responsible for all course material in the new (recycled) class.

j. Relief Actions. Students must attend all class sessions, complete all assignments, and conduct themselves in a manner expected of a Soldier or Noncommissioned Officer. The 305th MI Bn Commander will review the recommendation of the Instructor, the 35F Course OIC/NCOIC, and the student's Chain of Command. Only the 305th MI Bn Commander may relieve Soldiers from the course for failing to meet academic standards or administrative reasons, which include misconduct.

(1) **Academic Relief.** Academic relief occurs when the Soldier fails to meet the academic standards set forth in this SEP.

(2) **Administrative Relief.** Administrative relief occurs under circumstances, which do not merit academic relief, but which, otherwise support one or more of the following conclusions:

(a) The Soldier's personal conduct is such that the Soldier's continuation in the course is not justified.

(b) The Soldier's continuation in the course will be counter productive to the interests of other Soldiers in the class.

(c) It is extremely unlikely that the Soldier can successfully meet the standards established for graduation. Examples of circumstances that may serve as a basis for administrative relief include, but are not limited to, the following:

1) Misconduct. Relief for misconduct occurs when the Soldier engages in conduct or behavior that violates law, regulation, or policy (see paragraph 4a of this SEP). No formal adjudication of guilt by a military or civilian court or by a commander under Article 15, UCMJ is necessary to support relief under this paragraph.

2) Exceeding the body fat standards of AR 600-9, or fails to pass APFT IAW AR 350-1.

(d) Based upon the circumstances of the case, the 305th Battalion Commander may direct several personnel actions to include:

- 1) Reassignment for specific MI MOS training.
- 2) Reassignment for training in another MI MOS of the Soldier's choosing (based on Soldier's qualifications and the needs of the Army).
- 3) Reassignment for training in a specific non-MI MOS or CMF.
- 4). Reassignment for training in another MOS and CMF of the Soldier's choosing (based on Soldier's qualifications and the needs of the Army).
- 5) Return to parent unit (if TDY and return) or follow-on assignment IAW the needs of the Army (if TDY en route).
- 6) Separation from active duty; termination of active duty training, or other action as appropriate.

(e) **Returning Students.** Soldiers returning to the course after an administrative break in training of six months or less may be readmitted IAW TRADOC priority fill standards at the same point in the course they achieved previously. Soldiers with a break greater than six months will be evaluated for MOS proficiency through testing and may be admitted to the course IAW TRADOC priority fill standards at a point determined by the results of testing.

(3) **Processing Relief Actions and Appeals.** The 35F NCOIC will initiate all relief actions and process them through the appropriate Company to 305th MI BN according to the standards found in AR 350-1, TRADOC Regulation 350-18 and Fort Huachuca Memorandum 600-8. Soldiers awaiting a decision on a relief action will remain in the class and participate fully in all training events except tests. If a Soldier's conduct or demeanor is disruptive to the other Soldiers, immediate removal is permissible. That decision rests with the 35F Course OIC and the appropriate Company Commander.

4. **Counseling.** Instructors will conduct periodic formal counseling sessions with Soldiers throughout the course to review academic progress and discuss professional development. Additionally, instructors will complete a counseling form, DA Form 485E-R-E, for every Soldier with sustained poor performance. For the purposes of this SEP the term "negative" counseling relates to counseling due to unacceptable behavior or conduct, and not academic issues such as test failures.

a. Instructors will formally counsel Soldiers who fail to meet academic standards or if they fail to comply with the Department of Defense Directive 5500.7, Standards of Conduct.

b. Instructors will formally counsel Soldiers who fail to be at their appointed place of duty on time. Soldiers who show a pattern of lateness may be subject to UCMJ or other Administrative action or considered for relief by the Battalion commander.

c. Instructors will formally counsel Soldiers who fail a section or module of a performance based evaluation or a performance evaluation. The Soldier must attend all mandatory remedial training, and will be given only one retest for a failed evaluation (see Paragraph 3f of this SEP).

d. Students will be counseled not to acquire or provide unauthorized test assistance before, during, or after any test, except as instructed. Students will report any unauthorized test assistance (before, during, or after test administration) of which they are knowledgeable to their course instructors or the next leader in their chain of command.

5. Academic Evaluation Reports (AER). All MOS-T Soldiers will receive a DA 1059, Academic Evaluation Report (AER), IAW AR 623-3, paragraph 3-52 and TRADOC Regulation 350-6, paragraph 3-9, 3-26, Appendix F. The instructor will evaluate the Soldier's academic performance and record it on a counseling statement and on the Academic Evaluation Report (AER). All duties and responsibilities at the Company and in the classroom may be used to create bullets on the AER. Evaluation ratings are earned according to the following:

a. Performance Summary, AER Block 11.

(1) "Exceeded Course Standards." Soldier's whose overall course achievement is significantly above the standards of the course. This is limited to the top 20% of the class IAW DA Pam 623-3. To exceed course standards, at a minimum a Soldier must:

- (a) Earn 4 "SUPERIOR" ratings, and no "UNSATISFACTORY" ratings in block 12 of the AER.
- (b) Receive no negative counseling statements.
- (c) Meet height and weight standards IAW AR 600-9.
- (d) Meet APFT standards IAW AR 350-1 and FM 21-20.

(2) "Achieved Course Standards." Soldiers who achieve overall acceptable course standards. To achieve course standards, the Soldier must:

- (a) Earn at least a "SATISFACTORY" rating in each rated item listed in Block 12 of the AER.
- (b) Receive no more than two negative counseling statements.
- (c) Meet height and weight standards IAW AR 600-9.
- (d) Meet APFT standards IAW AR 350-1 and FM 21-20.

(3) "Marginally Achieved Course Standards." Soldier's who achieve with difficulty, the minimum acceptable course standards. A Soldier will marginally achieve course standards if any of the following apply:

- (a) Receive no more than four negative counseling statements.
- (b) Meet height and weight standards IAW AR 600-9.
- (c) Meet APFT standards IAW AR 350-1 and FM 21-20.

(4) "Failed to Achieve Course Standards." A Soldier will fail to achieve course standards if any of the following apply:

- (a) Earns a final "UNSATISFACTORY" rating in any rated area listed in block 12 of the AER. If a Soldier falls into this category, a recommendation for academic relief will be forwarded thru the appropriate Company Commander, to the 305th MI Bn Commander for relief consideration.
- (b) Receive five or more negative counseling statements.
- (c) Fail to meet height and weight standards IAW AR 600-9, paragraph 3-40f.

- (d) Fail to meet APFT standards IAW AR 350-1 and FM 21-20 (reference TRADOC Reg. 350-6 paragraph 4-3 c (4)).

b. **Demonstrated Abilities, AER Block 12:**

(1) Item 12a - Written Communication:

(a) **SUPERIOR** – a Soldier may receive a "SUPERIOR" rating if he/she earns a minimum passing score of 20% above the minimum passing requirement on all initial evaluations IAW the evaluation sheets used to evaluate written communication skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(b) **SATISFACTORY** – a Soldier may receive a "SATISFACTORY" rating if he/she earns at least a final minimum passing score IAW the evaluation sheets, used to evaluate written communication skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(c) **UNSATISFACTORY** – a Soldier may receive an "UNSATISFACTORY" rating and be recommended for relief from the course if he/she fails to meet the minimum passing score IAW the evaluation sheets, used to evaluate written communication skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(2) Item 12b - Oral Communication:

(a) **SUPERIOR** - a Soldier may receive a "SUPERIOR" rating if he/she earns a minimum passing score of 20% above the minimum passing requirement on all initial evaluations IAW the evaluation sheets used to evaluate oral communication skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(b) **SATISFACTORY** – a Soldier may receive a "SATISFACTORY" rating if he/she earns at least a final minimum passing score IAW the evaluation sheets, used to evaluate oral communication skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(c) **UNSATISFACTORY** – a Soldier may receive an "UNSATISFACTORY" rating and be recommended for relief from the course if he/she fails to meet the minimum passing score IAW the evaluation sheets, used to evaluate oral communication skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(3) Item 12c - Leadership Ability:

(a) **SUPERIOR** – A Soldier may earn a "SUPERIOR" rating if while participating in the day-to-day activities as a student and/or while serving in an assigned student leadership position demonstrates "Superior" Army leadership abilities and characteristics. All MOS-T Soldiers will be counseled on the minimum standards required to earn "SUPERIOR" on their DA 1059 (AER) for Leadership. Other such abilities and characteristics are those outlined in FM 7-22.7, The Army Noncommissioned Officer Guide, Ch. 3, Leadership, 3-6 - 3-21, and FM 6-22, Army Leadership, Appendix A, Leader Attributes & Core Leader Competencies, in the categories of Values, Attributes, Skills, and Actions (Be, Know, Do). Additionally, the soldier may receive no written counseling statements for failure to practice the Be, Know, Do principles of Army Leadership to be eligible for a "SUPERIOR" rating.

(b) **SATISFACTORY** – A Soldier may earn a "SATISFACTORY" rating if while participating in the day-to-day activities as a student and/or while serving in an assigned student leadership position demonstrates adequate Army leadership abilities and characteristics. Such abilities and characteristics are those outlined in FM 7-22.7, The Army Noncommissioned Officer Guide, Ch. 3, Leadership, 3-6 - 3-21, and FM 6-22, Army Leadership, Appendix A, Leader Attributes & Core Leader Competencies, in the categories of Values, Attributes, Skills, and Actions (Be, Know, Do). Additionally, the Soldier may receive

no more than one written counseling statement for failure to practice the Be, Know, Do principles of Army Leadership.

(c) **UNSATISFACTORY** – A Soldier may earn an "UNSATISFACTORY" rating and be recommended for relief from the course if while participating in the day-to-day activities as a student and/or while serving an assigned student leadership position fails to demonstrate adequate Army leadership abilities and characteristics. Such abilities and characteristics are those outlined in FM 7-22.7, The Army Noncommissioned Officer Guide, Ch. 3, Leadership, 3-6 – 3-21, and FM 6-22, Army Leadership, Appendix A, Leader Attributes & Core Leader Competencies, in the categories of Values, Attributes, Skills, and Actions (Be, Know, Do). In the event that a Soldier receives a second written counseling statement for failure to practice the Be, Know, Do principles he/she will be deemed to be an "Unsatisfactory" performer for Leadership Ability.

(4) Item 12d - Contribution to Group Work:

(a) **SUPERIOR** – A Soldier may earn a "SUPERIOR" rating if while participating in the day-to-day activities as a student and/or while serving in an assigned student leadership position demonstrates "Superior" efforts to their team accomplishing assigned group work IAW the standards provided by the respective instructor. Other such efforts, abilities and characteristics are those outlined in FM 7-22.7, The Army Noncommissioned Officer Guide, Ch. 3, Leadership, and FM 6-22, Army Leadership, Appendix A, Leader Attributes & Core Leader Competencies, in the categories of Values, Attributes, Skills, and Actions (Be, Know, Do). Additionally, the soldier may receive no written counseling statements for failure to contribute to group work or the dynamic of group efforts to be eligible for a "SUPERIOR" rating.

(b) **SATISFACTORY** – A Soldier may earn a "SATISFACTORY" rating if while participating in the day-to-day activities as a student and/or while serving in an assigned student leadership position demonstrates adequate efforts to their team accomplishing assigned group work IAW the standards provided by the respective instructor. Such efforts, abilities and characteristics are those outlined in FM 7-22.7, The Army Noncommissioned Officer Guide, Ch. 3, Leadership, and FM 6-22, Army Leadership, Appendix A, Leader Attributes & Core Leader Competencies, in the categories of Values, Attributes, Skills, and Actions (Be, Know, Do). Additionally, the Soldier may receive no more than one written counseling statement for failure to contribute to group work or the dynamic of group efforts.

(c) **UNSATISFACTORY** – A Soldier may earn an "UNSATISFACTORY" rating and be recommended for relief from the course if while participating in the day-to-day activities as a student and/or while serving in an assigned student leadership position fails to demonstrate accomplishment of assigned group work or fail to participate towards the completion of assigned tasks. Such abilities and characteristics are those outlined in FM 7-22.7, The Army Noncommissioned Officer Guide, Ch. 3, Leadership, and FM 6-22, Army Leadership, Appendix A, Leader Attributes & Core Leader Competencies, in the categories of Values, Attributes, Skills, and Actions (Be, Know, Do). In the event that a Soldier receives a second written counseling statement for failure to contribute to group work or the dynamic of group efforts, he/she will be deemed to be an "Unsatisfactory" performer for Contribution to Group.

(5) Item 12e - Research Ability:

(a) **SUPERIOR** – a Soldier may receive a "SUPERIOR" rating if he/she earns a minimum passing score of 20% + above the minimum passing requirement on all initial evaluations IAW the evaluation sheets used to evaluate research ability, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(b) **SATISFACTORY** – a Soldier may receive a "SATISFACTORY" rating if he/she earns at least a final minimum passing score IAW the evaluation sheets, used to evaluate research ability skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

(c) **UNSATISFACTORY** –a Soldier may receive an "UNSATISFACTORY" rating and be recommended for relief from the course if he/she fails to meet the minimum passing score IAW the evaluation sheets, used to evaluate research ability skills, as outlined in paragraph 2, Individual Course Examinations & Performance Objectives, of this SEP.

6. Student Grievances and Redress. The following policies and procedures have been established to protect Soldiers' rights and to rectify inconsistencies in the evaluation of Soldier performance.

a. Grievances that are purely academic in nature must first be discussed with the Senior Faculty Advisor, then the 35F1O Course NCOIC whose decision is normally final. In cases where discrimination or violation of policy may be involved, the Soldier should use the chain of command up to the 305th MI BN Commander to seek resolution of any, and all, issues.

b. All student rebuttals will be in writing, and must be submitted to the 35F1O Course NCOIC within 48 hours of the initial recycle/relief notification IAW FH Memorandum 600-8.

c. A Soldier may seek the assistance of the Inspector General (IG), Judge Advocate General (JAG) and Unit Chaplain at any time. The Soldier will inform their chain of command if they desire to see any of these agencies during duty time.

7. Student Academic and Incentive Awards

a. "Skill, Tough, Ready Around the Clock" (STRAC) Program.

1. Purpose: STRAC is a program designed to recognize students who excel in the TOTAL SOLDIER concept by exceeding course standards and military standards. The STRAC program is jointly administered by the 35F1O OIC and the respective training company commander IAW 305^W MI Battalion Policy. Soldiers completing all three requirements of the STRAC award will be recommended by their Platoon Sergeant or Drill Sergeant for an Army Achievement Medal (AAM).

2. Components of the STRAC Award:

a. Skill

i. "S" is achieved by Soldiers who attain academic excellence in their course of instruction. Their final grade point average (GPA) has placed them in the top 10 percent of all graduates in their respective classes. A 35F1O soldier requires a minimum GPA of 94% to be eligible for the "S" portion of the STRAC award.

ii. A Soldier that attains the necessary GPA to qualify for the 'S' Portion is recommended for a Battalion Certificate of Achievement, unless that Soldier completes all three portions of the STRAC criteria thereby being recommended for an AAM.

b. Tough

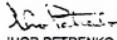
i. "T" is achieved by Soldiers who attain at least 90 points or higher in each event on the Army Physical Fitness Test (APFT). An extended score is not used for this evaluation.
ii. Soldiers who meet criteria for the "T" portion will be awarded the Army Physical Fitness Badge.

c. Ready Around the Clock

i. "RAC" is awarded to those Soldiers who appear before a board of NCOs and demonstrate high standards of military bearing, appearance and exceptional knowledge of military subjects and current events.
ii. The RAC Board will select Soldiers for recognition under the STRAC program. Candidates must meet the following qualifications prior to appearing before the board.

1. Maintain an academic GPA of 94% or higher

2. Scored at least 270 points on their most current APFT
 3. Demonstrate exceptional individual achievement of non-academic IET standards such as: basic Soldiering, warrior tasks and drills, and volunteer efforts.
 4. Have no record of disciplinary actions while assigned to the 305th MI BN as verified by their chain of command (PSG, Drill Sergeant, 1SG).
 - iii. Soldiers who are recommended by the RAC Board will be awarded a Company Certificate of Achievement.
- 8. Challenging Training.** There is no test-out policy within the 35F1O, Intelligence Analyst Course.
- 9. Ability Based Training Program (ABTP).** The ABTP is an optional accelerated training program designed to reduce training Time on Station (TOS) for experienced student NCOs and Warrant Officers (WO). The ABTP reflects an intensive, compressed training schedule employing low Instructor to Student ratios. The ABTP is offered subject to the availability of required resources.
- a. Students who meet the following criteria are eligible to participate:
 1. Volunteer
 2. Rank: SSG or above
 3. Military Education: BNCO, Battle Staff, or above and WO equivalent
 4. Recommendation of the 35F1O Course NCOIC
 5. Approval of the 35F1O Course OIC
 - b. Participants are subject to the same academic and administrative provisions specified in this SEP.
-With the exception of students recycled from ABTP.
- 10. POC:** 35F1O Committee Chief, CW3 Hess, James, Phone (520) 538-6428.



IHOR PETRENKO
LTC, AV
Commanding

STUDENT ACKNOWLEDGMENT and CONSENT TO RELEASE

I have received a copy of this Student Evaluation Plan for the 243-35F1O (V10) Tactical Intelligence Analyst Course 35F1O and I understand the content and requirements to graduate from this course. I understand that my performance at the 35F1O course may affect my future assignments.

Date: _____

Student Signature: _____

Printed Name: _____

Class number: _____

Signature of the Instructor: _____

(Note: This acknowledgment must be completed by the student and instructor and ultimately filed in the student's academic file)

UNITED STATES OF AMERICA

v.

Manning, Bradley E.

PFC, U.S. Army,

HHC, U.S. Army Garrison,

Joint Base Myer-Henderson Hall

Fort Myer, Virginia 22211

)

)

)

)

)

)

)

)

Prosecution Motion

for Preliminary Ruling on
Admissibility of Evidence
(Business Records)

Enclosure 7

22 June 2012

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS

I, Theresa Robinson attest that I am employed by Defense Information Systems Agency (DISA), Chambersburg, PA 17201 and that my official title is Management Analyst. I am a custodian of records for DISA Field Security Operations (FSO), Chambersburg, PA 17201. I certify that the attached records are the originals or true and accurate copies of the originals. I am the custodian of the attached records consisting of 2 CD(s). I have provided the following:

- DoD IA Awareness version 7 (dated October 2008)
- DoD IA Awareness version 8 (dated October 2009)

Furthermore, the attached documents were made by, or from, information transmitted by a person with knowledge of the events recorded, were made at or near the time of the events recorded. We create and maintain these documents in the regular course of business as a regular practice.

This certification is intended to satisfy Military Rule of Evidence 902(11).

Theresa Robinson
(Signature)

Theresa Robinson _____
(Printed Name)

13 July 2011 _____
(Date)

1 Overcash Avenue, Chambersburg, PA 17201 _____
(Address)

717-267-5696 _____
(Phone)

Prosecution Exhibit 7
(Attachments)
have been entered into
the record as CD/DVDs
and will be maintained
with the original
Record of Trial

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)

)
)
)
)
)

Prosecution Motion

for Preliminary Ruling on
Admissibility of Evidence
(Business Records)

Enclosure 14

22 June 2012

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

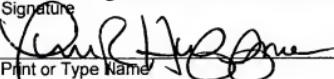
1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. It was the regular practice of the business activity to make the records; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

INDOC - COMINT - 29 Jan 10.pdf (1 Page)
JCAVS Report - 26 May 2010.pdf (2 Pages)
SCI Packet - Jan 2009.pdf (22 Pages)

Organization

10TH MOUNTAIN Division (LI)

Signature	Date
	08 FEB 2012
Print or Type Name	Title
TINA R. HUFFMAN	SCI PROGRAM MANAGER
Business Telephone	Business Address
315-772-7163	P-10000, 10TH MTN DIV PR FORT DRUM, NY 13602 C/O SSO

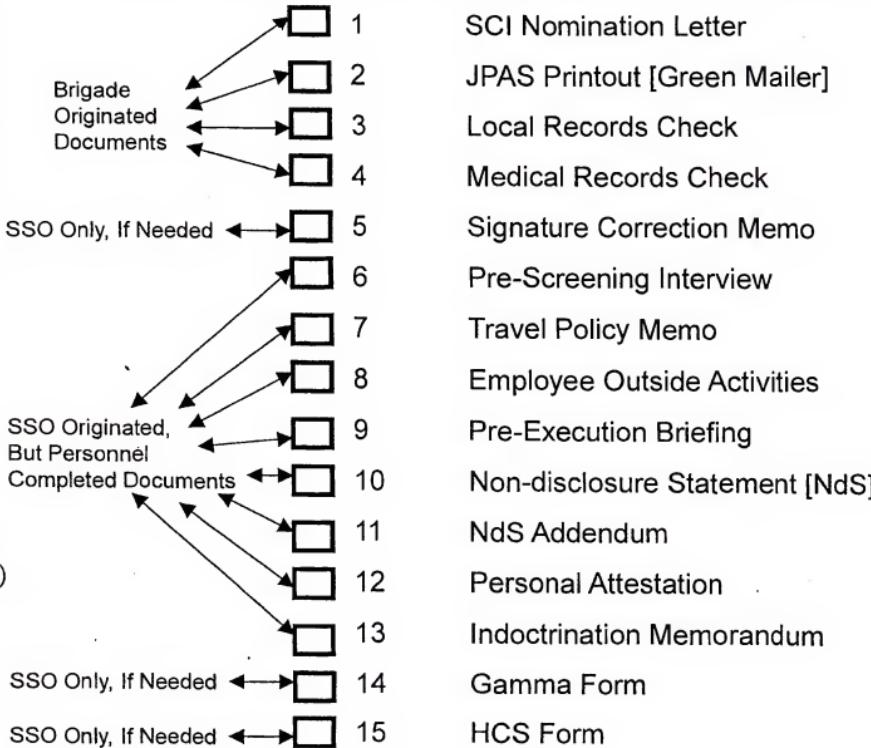
Subscribed and sworn to before a notary public, this 8 day of Feb, 2012.

Notary Public	My commission expires on:
	12-19-2015

Holly A. Parker
No. 01P16252938

10th Mountain Division Special Security Office SCI Indoctrination Checklist

0028-10-CID221-10117



0028-10-CDD221-10117

11. Date (YYYYMMDD)
20090122

REQUEST FOR PRIVATE MEDICAL INFORMATION

For use of this form, see AR 40-66; the proponent agency is the OTSG

2. Patient's Name and SSN

Bradley E. Manning
[REDACTED]

3. Medical Treatment Facility (Name and Location)

Connor Troop Medical Clinic

4. Reason for Request.

In accordance with AR380-67, paragraph 2-200, the individual listed above requires a medical records review..

5. Private Medical Information Sought (Specify dates of hospitalization or clinic visits and diagnosis, if known)

Copies of health record documents, or complete summaries, including dates and details, which may have a bearing on the individual's suitability to hold a security clearance. The review of medical records should include, but not be limited to:

1. Habitual or excessive use of intoxicants.
2. Drug abuse.
3. Sexual perversion.
4. Any illness, mental condition, instability, nervous condition or history of fainting, seizure, or loss of consciousness which, with due regard to the transient or continuous effort of the condition, may in the opinion of competent medical authority cause significant defect in the judgment or reliability of the individual.
5. History of treatment, rehabilitation or recuperation from those conditions previously indicated.

A MEDICAL OPINION CONCERNING THE INDIVIDUAL'S SUITABILITY TO HOLD A SECURITY CLEARANCE IS NEITHER SOLICITED NOR DESIRED. THAT DETERMINATION WILL BE MADE BY U.S. ARMY SECURITY ADJUDICATORS BASED UPON ALL AVAILABLE INFORMATION.

6. Requestor's Name, Title, Organization and SSN.

Kyle J. Balonek, Brigade Security Manager
HHC, 2BCT 10th MTN DIV
108-72-1513

FOR USE OF MEDICAL TREATMENT FACILITY ONLY.

7. Check applicable box.

 Approved Disapproved (State reason for disapproval)

8. Summary of Private Medical Information Released.

CHECK AS APPROPRIATE:

- No adverse medical information found.
- Copies of adverse medical information is attached.
- A summary of adverse medical information follows (continue on attached sheet if necessary).

9. Signature of Approving Official

DA FORM 4254, FEB 2003

10. Date (YYYYMMDD)

20090124

FOR OFFICIAL USE ONLY
DA FORM 4254, NOV 91, IS OBSOLETE.

APD PE v1.01

SCI PRE-INDOCTRINATION SCREENING INTERVIEW

1. The following questions will be answered by the nominee. Responses to these questions should cover the period of time from the date you last had a screening interview, special background investigation [SBI], or single scope background investigation [SSBI].

a. Has there been any change in your marital status? NO

b. Has there been any change in the citizenship of your spouse? NO

c. Have you had any involvement with either civilian or military law enforcement agencies? [i.e. traffic tickets, article 15's, letter of reprimands, etc.]? NO

d. Have you had any treatment or experiences involving stress, nervous disorders or counseling? NO

e. Have you experimented with or otherwise used any controlled substances [i.e. marijuana, cocaine, crack, etc.]? NO

f. Have you had any alcohol related incidences [i.e. DUI/DWI, drunk in public, etc.]? NO

g. Have you experienced any financial problems [i.e. bankruptcy, accounts in collections, bounced checks, etc.]? NO

h. Have you formed any close associations with people or organizations of foreign nationality or of questionable loyalty to the US or its allies? NO

i. Are there any incidents which might make you subject to blackmail [i.e. fraud, extra-marital affairs, etc.]? NO

Name: MANNING, BRADLEY EDWARD

Signature: Date: 22 JAN 08



0028-10-CID221-10117

DEPARTMENT OF THE ARMY
HEADQUARTERS, 10TH MOUNTAIN DIVISION (LIGHT INFANTRY) AND FORT DRUM
FORT DRUM, NEW YORK 13602-5000

REPLY TO
ATTENTION OF

AFZS-IN-ACoSG2

DATE 22 JAN 09MEMORANDUM FOR 10TH MTN Special Security Office [SSO]

SUBJECT: SCI Security Awareness and Defense Travel Briefing.

1. References:

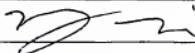
- a. DoD S-5105.21-M-1, SCI Admin Security Manual, AUG 98
 - b. AR 380-28, DA Special Security System, AUG 97
2. IAW references above, I have read the SSO 10th MTN "security awareness briefing" and understand the policy and procedures for the use and protection of Sensitive Compartmented Information Facility [SCIF]. Any specific questions concerning the use of protection of SCI not outlined in the briefing will be directed to the SSO for clarification.
3. I have also reviewed the Defense Travel Security Briefing and understand my responsibility to report all official or unofficial foreign travel to my security manager or the special security office.
4. As outlined in reference A above, my review of these documents meets the annual requirement for security Awareness and Defense Travel Briefing for SCI-Indoctrinated personnel.
5. A copy of this memorandum will be maintained in the SSO for two years after the date of my SCI debrief or departure from this organization.
6. POC for this action is the 10th MTN SSO at DSN 772-8084

Name: MANNING, BRADLEY EDWARDSignature: 22 3

M. Employee Outside Activities. Potential conflicts with an individual's responsibility to protect SCI material may arise from outside employment or other outside activity from contact or association with foreign nationals. In cases where such employment or association has resulted in a suspected or established compromise of SCI, the local SCI security official and supporting Counter-Intelligence activity must be advised immediately. Involvement in non-U.S. government employment or activities that rise potential conflicts with an individual's responsibility to protect classified information is of security concern and must be evaluated by an ASI security official to determine whether the conflict is of such a nature that SCI access should be denied or revoked. Individuals who hold or are being considered for SCI access approval must report in writing to the local SCI security official any existing or contemplated outside employment or activity that appears to meet the criteria listed below. In addition, initial or updated personal history statements must include details of outside employment or activities.

1. Employments that must be reported includes compensated or volunteer service with any foreign national; with a representative of any foreign interest; or with any foreign, domestic or international organization or person engaged in analysis, discussion, pr publication of material on intelligence, defense, or foreign affairs.
2. Continuing association with foreign nationals must be reported.
3. When an individual's outside employment or activity raises doubt as to an individual's willingness or ability to safeguard classified information, he or she will be advised that continuing that employment or activity may result in withdrawal of SCI access and be given an opportunity to discontinue. If the individual terminates the outside employment or activity of security concern, his or her SCI access approval may be continued provided this is otherwise consistent with national security requirements.
4. DoD SCI indoctrinated individuals will have paragraph M made available to them for reading during SCI Indoctrination. Annual security education will advise individuals to report in writing to their local SCI security officer any existing or contemplated outside employment or activity that appears to meet the above criteria. Written reports must be submitted before accepting outside employment or activity.

Name: MANNING, BRADLEY EDWARD

Signature: 

Date: 22 JAN 08

PRE NONDISCLOSURE EXECUTION BRIEFING

Sensitive Compartmented Information [SCI] is data about sophisticated technical systems for collecting intelligence and information collected by those systems. SCI systems require a large number of people to research, develop, build, and operate the collection systems. The products of these systems are analyzed and produce accurate, detailed intelligence by senior planners and policy makers.

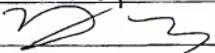
Communications Intelligence [COMINT], as defined by 18 U.S.C. 798, is the classic example of SCI, and normally is derived from intercepted communications. The unauthorized disclosure of COMINT can reveal to the target countries which of its messages are being intercepted and which ones are being read. If the targeted country implements countermeasures, no further intelligence can be expected from that source and by that method. More devastating than countermeasures are deception operations which provide misleading or false data that can result in us U.S. foreign and defense policies based on misleading data. The cost to replace such systems is enormous.

SCI systems encompass activities and information of extraordinary sensitivity and fragility requiring extensive security. Security for SCI is based on restricting access to person who has a clearly established official need for that information, and who meet rigorous and stringent personnel security criteria. Persons cleared for confidential, secret, or even top secret information are not eligible by virtue of those clearances for access to SCI. Furthermore, a person does not have access to SCI because of rank or position.

The security of SCI depends on distinctive security markings, restricted handling and dissemination controls, segregating information and programs to further restrict access, and maintaining SCI material found in "Control Facilities" which have a stringent physical and procedural barrier and secure means of transmitting SCI.

Persons indoctrinated for SCI accept certain responsibilities and restrictions in a most explicit way. As a condition of access, an individual signs a nondisclosure agreement which is contractual agreement between the government and the individual. This agreement should be read carefully before signing because it states obligations imposed on the individual and the government. Also, because of an individual's knowledge and access to SCI an individual may be denied travel to activities which are deemed Hazardous. Willful disclosure of SCI to unauthorized individuals, compromise or security violations constitute criminal or administrative offenses that may result in prosecution or administrative action. Once indoctrinated it is individual's responsibility to become knowledgeable of the security procedures and practices for SCI.

Name: MANNING, BRADLEY EDWARD

Signature: 

Date: 22 JAN 09

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE STATEMENT

PRIVACY ACT STATEMENTAUTHORITY: EO 9397, November 1943 (SSN).PRINCIPAL PURPOSE(S): The information contained herein will be used to precisely identify individuals when it is necessary to certify their access to sensitive compartmented information.ROUTINE USE(S): Blanket routine uses, as published by Defense Intelligence Agency in the Federal Register.DISCLOSURE: Voluntary; however, failure to provide requested information may result in delaying the processing of your certification.SECTION AAn Agreement Between MANNING, BRADLEY EDWARD and the United States.
(Printed or Typed Name)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or in the process of a classification determination under the standards of Executive Order 12356 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government. **BEM**

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements. **BEM**

3. I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion. **BEM**

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI in an unauthorized fashion. **BEM**

4. *(Continued)* have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted. **BEM**

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 set forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt. **BEM**

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation. **BEM**

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys' fees incurred by the United States Government may be assessed against me if I lose such action. **BEM**

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a

8. (Continued) court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code. **BEM**

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all the conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter. **BEM**

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency. **BEM**

11. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations, rights, or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act

11. (Continued) (governing disclosure of illegal, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling. **BEM**

12. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12356, as amended, so that I may read them at this time, if I so choose. **BEM**

13. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement. **BEM**

14. This Agreement shall be interpreted under and in conformance with the laws of the United States. **BEM**

15. I make this Agreement without any mental reservation or purpose of evasion. **BEM**

16. TYPED OR PRINTED NAME (Last, First, Middle Initial) MAUNING, BRADLEY E	17. GRADE/RANK/SVC E3/PFC	18. SOCIAL SECURITY NO. 445-98-9504	19. BILLET NO. (Optional)
20. ORGANIZATION HHC, SA 2 RCT 10TH MTN DIV	21. SIGNATURE 	22. DATE SIGNED (YYMMDD) 090122	

FOR USE BY MILITARY AND GOVERNMENT CIVILIAN PERSONNEL

SECTION B

The execution of this Agreement was witnessed by the undersigned, who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

23. TYPED OR PRINTED NAME (Last, First, Middle Initial) STEALY, LUCILLE	24. ORGANIZATION HHC 2 RCT 10th MTN DIV (CL)	25. SIGNATURE 	26. DATE SIGNED (YYMMDD) 090122
---	---	-------------------	---

FOR USE BY CONTRACTORS/CONSULTANTS/NON-GOVERNMENT PERSONNEL

SECTION C

The execution of this Agreement was witnessed by the undersigned.

27. TYPED OR PRINTED NAME (Last, First, Middle Initial)	28. ORGANIZATION
29. SIGNATURE	30. DATE SIGNED (YYMMDD)

SECTION D

This Agreement was accepted by the undersigned on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

31. TYPED OR PRINTED NAME (Last, First, Middle Initial)	32. ORGANIZATION
33. SIGNATURE	34. DATE SIGNED (YYMMDD)

10/91
e

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 841, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE 	DATE 17 SEP 08	SOCIAL SECURITY NUMBER (See Notice below) 445-98-9504
--	-------------------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)
(Type or Print)

Manning, Bradley Edward
10100 N. Riva Ridge LP
FT Drum, NY 13602

WITNESS	ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE 	DATE 17 Sep 08	SIGNATURE
NAME AND ADDRESS (Type or print) Balonck, Kyle J 10100 N. Riva Ridge Loop FT. Drum, NY 13601	NAME AND ADDRESS (Type or print) Stark, Loren J 10100 N. Riva Ridge Loop FT. Drum, NY 13601	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
-----------------------	------

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS
---------------------------------	----------------------

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to: 1) certify that you have access to the information indicated above or; 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (REV. 1-00)
APD PE v1.00

FOR OFFICIAL USE ONLY

Law Enforcement Specific



DEPARTMENT OF THE ARMY
HEADQUARTERS, 10TH MOUNTAIN DIVISION (LIGHT INFANTRY) AND FORT DRUM
FORT DRUM, NEW YORK 13602-5000

REPLY TO
ATTENTION OF

AFZS-LF-1

DATE 22 JAN 09MEMORANDUM FOR 10TH MTN Special Security Office [SSO]

SUBJECT: Personal Attestation upon the Granting of Security Access.

1. I, BRADLEY EDWARD MANNING, accept the responsibilities associated with being granted access to Classified National Security Information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and the need to know. I further understand that, in being granted access to classified information, a special confidence and trust has been placed in me by the United States Government.
2. This form will be placed in the individuals security folder and maintained IAW AR 380-67

Name: MANNING, BRADLEY EDWARDSignature:

Witness:

Name: Stark, Loren J. 2LT

Signature:

307A
25 01/09
P



DEPARTMENT OF THE ARMY
HEADQUARTERS, 10TH MOUNTAIN DIVISION (LIGHT INFANTRY) AND FORT DRUM
FORT DRUM. NEW YORK 13602-5000

REPLY TO
ATTENTION OF

AFZS-IN-ACoSG2

DATE 22 JAN 09MEMORANDUM FOR 10TH MTN Special Security Office [SSO]

SUBJECT: Personal Attestation of Receiving Access Card and/or Picture Badge.

1. I, MANNING, BRADLEY EDWARD, have been issued

A 10th Mountain Division [LI] SCIF Access Card with personalized PIN Code. I understand that this card and pin code are accountable items and can not be given to, or shared with, any other person. I understand all transactions involving this SCIF Access Card are to go through the SSO directly, and immediately. I understand that returning the SCIF Access Card to the SSO is part of the mandatory out-processing requirements.

A 10th Mountain Division [LI] Picture Badge. I understand that this Badge is to be displayed in SCIF areas only, or T-SCIF areas during exercises. I understand that the Picture Badge is only a reflection of the Access Roster maintained by the SSO and is to be returned to the SSO as part of the mandatory out-processing requirements.

2. I understand failure to comply will delay in-processing gaining unit and may complicate obtaining accesses through gaining unit.
 3. This form will be placed in the individuals security folder and maintained IAW AR 380-67

Name: MANNING, BRADLEY EDWARD

Signature:

10/09
KMC
P



DEPARTMENT OF THE ARMY
HEADQUARTERS, 10TH MOUNTAIN DIVISION (LIGHT INFANTRY) AND FORT DRUM
FORT DRUM. NEW YORK 13602-5000

REPLY TO
ATTENTION OF

AFZS-IN-ACoSG2

DATE 22 JAN 09

MEMORANDUM FOR 10TH MTN Special Security Office [SSO]

SUBJECT: Special Intelligence [SI] and Talent Keyhole [TK] Briefings

1. I, BRADLEY EDWARD MANNING, acknowledge that the 10th MTN DIV [LJ] SSO has made available to me: The Special Intelligence [SI] and Talent Keyhole [TK] briefings during my Sensitive Compartmented Information [SCI] Indoctrination Briefing.
2. This form will be placed in the individuals security folder and maintained IAW AR 380-67

Name: MANNING, BRADLEY EDWARD

Signature:

Witness:

Name: STAKE, LOREN S

Signature:

**SENSITIVE COMPARTMENTED INFORMATION
indoctrination memorandum**

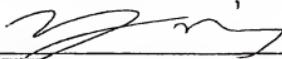
This memorandum records the fact that I was briefed on this date on the following Sensitive Compartmented Information (SCI) Special Access Program(s) (Use Unclassified Indicators Only):

Top Secret SCI ITk

Authority (optional):

The need for special protection of this material was made known to me, and I was reminded that my access to this material is governed by the terms of the SCI Nondisclosure Agreement that I signed.

Signature



Printed/Typed Name (Last, First, Middle Initial)

MANNING, BRADLEY E

Rank/Grade

PFC / E3

Date of Indoctrination
(YY, MM, DD)

090129

HHC 2BCT 10MNU DIV

Organization

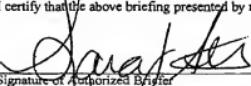
445 98 9504

SSN (See Notice Below)

Billet Number

I certify that the above briefing presented by me was in accordance with relevant SCI procedures.

Signature of Authorized Briefing Officer



Printed/Typed Name (Last, First, Middle Initial)

Alice, Sara J

G2-SSO

Organization

090129

Date of Briefing (YY, MM, DD)

Notice: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above. Although disclosure of your SSN is not mandatory, your failure to do so may delay the processing of such certification.

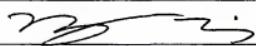
100-250-3
100-250-3

ADDENDUM
[To DD Form 1847-1]

Pursuant to Treasury, Postal Service, and General Government Appropriations Act of 1991; the following language shall be incorporated into and considered part of the attached Non-Disclosure-Agreement:

"These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order 12356, section 7211 of title 5, United States Code, [Governing disclosures to congress] Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act [governing disclosure to congress by members of the military]; section 2303 [b][8] of title 5, United States Code, as amended by the Whistleblower Protection Act [governing disclosures of illegality, waste, fraud, abuse of public health or safety threats]; the intelligence identities protection act of 1982 [50 USC 421 et seq.] [governing disclosures that could expose confidential government agents], and the statutes which protect against disclosure that may compromise the national security, including section 641,793,794,798 and 952 of Title 18, USC, and section 4[b]. the definitions, requirements, obligations, rights, sanctions and liabilities crated by said Executive Order and listed statuses are incorporated into this agreement and are controlling."

Name: MANNING, BRADLEY EDWARD

Signature: 

Date: 22 JAN 09

10 sep 10
KME

SENSITIVE COMPARTMENTED INFORMATION NO. 1301-001-0001

An Agreement Between

BRADLEY EDWARD MANNING

and the United States.

(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access information or material protected within Special Access Programs, hereinafter referred to in the Agreement as Sensitive Compartmented Information (SCI) have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in process of a classification determination u the standards of Executive Order 12958 or other Executive Order or statute. I understand and accept that by being granted access to SCI, special confid and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved access to it, and understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereina Department or Agency) that authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be S I further understand that I am obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access SCI, I hereby agree to be submitted for security review by the Department or Agency that last authorized my access to such information or material, a writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that pertain relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation with, or showing it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will set upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 3 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in my termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provide me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever, to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

4414 (EF)

(Replaces Form 4355
which is obsolete and
will not be used)FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Page 1 of 2

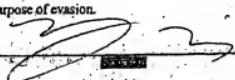
11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer made available Sections 793, 794, 798 and 752 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12958, as amended, so that I may read them at this time, if I so choose.

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code amended by the Military Whistleblowers Protection Act (governing disclosures to Congress by members of the Military); Section 2362(b)(8) of Title 18, United States Code, as amended by the Whistleblower Protection Act (governing disclosure of illegality, waste, fraud, abuse, or public health or safety threats); the Intelligence Identifications Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents and the statutes which protect agent disclosure which may compromise national security, including Section 641, 783, 794, 798, and 832 of Title 18, United States Code); and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

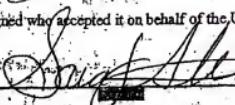
14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation or purpose of evasion.


28 JAN 09

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:


090129

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

HCS-P

(Special Access Programs by Initials Only)

SSN (See Notice Below)

Printed or Typed Name

Organization

10th MTN DIV

BRIEF

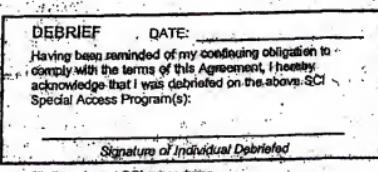
DATE:

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

DEBRIEF

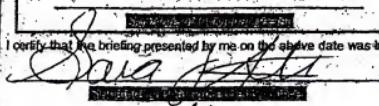
DATE:

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Program(s):


Signature of Individual Debriefed

I certify that the briefing presented by me on the above date was in accordance with the relevant SCI procedures.

064-100-14274
SSN (See Notice Below)


Sara Alicie
Printed or Typed Name

SSO 10th MTN DIV, FT Drum, NY

Organization (Name and Address)

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications, or determinations.

FOR OFFICIAL USE ONLY
Law Enforcement Services

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

MANNING, Bradley
(Name of Individual - Printed or typed)

AND THE UNITED STATES

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 14(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or lest granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from every position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, 1952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

U028 10-07221-1n117

10. These restrictions are consistent with and do not supersede, conflict with or otherwise affect the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identifications Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its Implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE 	DATE 17 SEP 08	SOCIAL SECURITY NUMBER (See Notice below) 445-98-9504
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or Print)		

Manning, Bradley Edward
10100 N. Riva Ridge LP
FT Drum, NY 13602

WITNESS	ACCEPTANCE		
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE 	DATE 17 Sep 08	SIGNATURE	DATE
NAME AND ADDRESS (Type or print) Balonek, Kyle J 10100 N. Riva Ridge Loop FT. Drum, NY 13601		NAME AND ADDRESS (Type or print) Stark, Loren J 10100 N. Riva Ridge Loop FT. Drum, NY 13601	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C., § 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to: 1) certify that you have access to the information indicated above or; 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (REV. 1-80)
APD PE v1.00

For Official Use Only
Law Enforcement
Sensitive

99/10.1

AFDR-BBA-IN

22 January 2009

MEMORANDUM TO Division Provost Marshal

SUBJECT: Request for Local Provost Marshal Records Check

1. Reference: AR380-67, Personnel Security Program, 9 Sep 88
2. In accordance with AR380-67, the individual listed below requires a local law enforcement records check. This check is to determine if the individual has a record of any derogatory information. This information will become a part of the individual's application for a personnel security clearance.
3. Request your office conduct this check and indicate below if there is a record of any derogatory information.

4. Individual Information:

NAME: Bradley E. Manning
 RANK: PFC
 UNIT: HHC 2BCT
 SSN: [REDACTED]

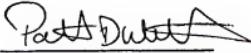


Kyle J. Balonek
 2BCT Personal Security Manager
 315-772-7346

FOR PROVOST MARSHAL USE ONLY

TO WHOM IT MAY CONCERN

- A. The above named individual does / does not (circle one) have derogatory information.
 B. The list of positive results is listed here.

NAMEOFFENSEDATEMPR-NO


PMO APPROVING AUTHORITY
P. Joseph F. Margrey
 Director, Enclg. Svcs.

FBI - G - 2000

Person Summary

MANNING, BRADLEY EDWARD

Person Category

Active Duty - Enlisted (USA)

SSN: [REDACTED]

Date of Birth: 1987 12 17

Open Investigation: N/A

Marital Status: N/A

PSQ Sent Date: N/A

Place of Birth: Oklahoma

Attestation Date: N/A

Citizenship: U.S. Citizen

Incident Report: N/A

NdA Signed: Yes

SF 713 Fin Consent Date: N/A

NdS Signed: No

SF 714 Fin Disclosure N/A

Date: N/A

Polygraph: N/A

Foreign Relation: 1, Mother, United Kingdom

PSQ SentRequest to Research/Upgrade EligibilityNon-SCI Access HistoryNdA History**Accesses**

Category	US Access	PSP	Suitability and Trustworthiness	Available Actions
Active Duty - Enlisted (USA)	Top Secret	No	IT: 3 Public Trust: N/A Child Care: N/A	Indoctrinate Non-SCI Debrief Non-SCI

Person Category Information

Category Classification: N/A

Organization: WBDAAA, 0010 IN HHC 02 HHC BDE LID, , FT DRUM, NY, 13602

Organization Status: N/A

Occupation Code: N/A

Separation Date: N/A

SCI SMO: N/A

Non-SCI SMO: 2ND BCT, SID, Level 6, 315-772-7346, kyle.balonek@us.army.mil

Servicing SMO: Yes

Grade: E3

Office Symbol: N/A

PS: N/A

Position Code: N/A

RNLTD: N/A

Arrival Date: N/A

Office Phone DSN: N/AOffice Phone Comm: N/A

TAFMSD: 2007 09 26

Separation Status: N/A

Proj. Departure Date: N/A

Interim: N/A

Proj. UIC/RUC/PASCODE: N/A

Report IncidentIn/Out ProcessRemarksSuspense DataInvestigation SummaryInvestigation History

0028-10-CID221-10117

SSBI from OPM, Opened: 2007 10 10 Closed 2008 01 15
ENAC from OPM, Opened: 2007 09 26 Closed 2007 10 02

Adjudication Summary**Adjudication History**

PSI Adjudication of SSBI OPM, Opened 2007 10 10, Closed 2008 01 15, determined Eligibility of SCI - DCID 6/4 on 2008 10 06 ArmyCCF
Interim SCI Adjudication of ENAC OPM, Opened 2007 09 26, Closed 2007 10 02, determined Eligibility of Interim SCI on 2007 10 17 ArmyCCF

External Interfaces**Perform SII Search****DCII**

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

10/26/2010
FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

<https://jpasapp.dsis.dod.mil/JPAS/JCAVSSelectAPersonServlet>

1/22/2009



DEPARTMENT OF THE ARMY
HEADQUARTERS, 2D INFANTRY BRIGADE COMBAT TEAM
10TH MOUNTAIN DIVISION (LIGHT INFANTRY)
FORT DRUM, NEW YORK 13602

0028-10-CID221-10117

AFZS-LF-I

22 January 2009

MEMORANDUM FOR SSO, 10th MTN Division

SUBJECT: Nomination for SCI Access

1. The following Individual requires access to SCI material:

NAME AND RANK:	Manning, Bradley E.
SSN, DOB, POB:	[REDACTED] 17 December 1987, San Diego, CA
POSITION:	35F, Intelligence Analyst
ORGANIZATION:	HHC, 2BCT 10th Mountain Division
EMAIL Address	bradley.manning@us.army.mil

2. Justification. PFC Manning is an Intelligence Analyst assigned to the S2 section 2BCT, 10th Mountain Division (LI). He requires a TS Clearance with access to SCI (SI/TK/G/HCS).

3. PFC Manning's requirement for TS/SCI is validated by the unit Security Manager and certified there are no known reasons why this individual should be denied access to SCI. Additionally, should any such information be discovered, it will be reported to the 10th MTN Division SSO immediately.

4. The point of contact for this memorandum is the undersigned at 772-7347.

LOREN J. STARK
2LT, MI
Brigade Security Manager

gNK
1/25/09
e

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY
CONFIDENTIAL//COMINT/XI~~

(U//FOUO) INDOCTRINATION FOR SENSITIVE SERIES COMINT

(U//FOUO)

1. (E) Certain communications intelligence, due to its unique or highly sensitive nature, is Published in GAMMA series reports and requires more restrictive handling than normal TOP SECRET Codeword Product.

(U//FOUO)

2. (E) In accordance with the community-wide criteria set forth in the Signals Intelligence Security Regulations (SISR), COMINT is placed in the GAMMA Series by the Director, NSA based on one or more of the following factors:

- a. Collection methods, when the dissemination of the information could reveal an unusually sensitive method or location.
- b. Analytic techniques, when the dissemination of the information could reveal an unusually sophisticated SIGINT technique.
- c. Security provisos, when a providing Agency (other than NSA) determines that restricted protection is necessary to protect a sensitive means of collection or when the existence or contents of the report could reveal the means of collection.
- d. Sensitive substantive content
- e. A sensitive target

3. (U//FOUO) Access to GAMMA COMINT requires special clearance.

(U)

4. (E) If used in any manner in other publication, memos, cables or briefings, GAMMA information must be identified by the caveat "GAMMA Controlled Item" and access to such materials may only be afforded to persons having the GAMMA clearance. GAMMA material is never used in normal COMINT series reports outside the GAMMA Control System.

(U//FOUO)

5. (E) GAMMA sensitive series COMINT produced by U.S. or second party cryptologic activities is easily recognized by the use of the appropriate GAMMA control caveat. Additionally, these items are identified in the COMINT serial.

EXAMPLE: G/O●/XXXX-99

I have read and understand this memo

Date: 29 JAN 09

Signature:

Print: MANNING, BRADLEY E.

~~CONFIDENTIAL//COMINT/XI~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

FOR OFFICIAL USE ONLY
Low Enforcement Sensitive

100-
100-
100-
100-
100-

Person Summary

MANNING, BRADLEY EDWARD**Person Category**

Active Duty - Enlisted (USA)

SSN: [REDACTED]

Date of Birth: 1987 12 17

Eligibility: SCI - DCID 6/4, 2008 10 06, DoD
CAF

Place of Birth: Oklahoma

Investigation: SSBI, 2008 01 15, OPM

Accesses

Category	US Access	Suitability and Trustworthiness	SCI
Active Duty - Enlisted (USA)	Top Secret	IT: 3 Public Trust: N/A Child Care: N/A	SI TK G HCS
			Access Number: N/A

Person Category Information**Category Classification:** N/A**Organization:** WBDAAA, 0010 IN HHC 02 HHC BDE LID, , FT DRUM, NY, 13602**Organization Status:** N/A**Grade:** E4**Interim:** N/A**External Interfaces**[Perform SII Search](#)

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Person Summary

MANNING, BRADLEY EDWARD**Person Category**

Active Duty - Enlisted (USA)

SSN: [REDACTED]

Date of Birth: 1987 12 17

Eligibility: SCI - DCID 6/4, 2008 10 06, DoD
CAF

Place of Birth: Oklahoma

Investigation: SSBI, 2008 01 15, OPM

Accesses

Category	US Access	Suitability and Trustworthiness	SCI
Active Duty - Enlisted (USA)	Top Secret	IT: 3 Public Trust: N/A Child Care: N/A	Yes

Person Category Information

Category Classification: N/A

Organization: WBAAA, 0010 IN HHC 02 HHC BDE LID, , FT DRUM, NY, 13602

Organization Status: N/A

Grade: E4

Interim: N/A

External Interfaces[Perform SII Search](#)

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)) Prosecution Motion

)) for Preliminary Ruling on
)) Admissibility of Evidence
)) (Business Records)

Enclosure 15

22 June 2012

PROSECUTION EXHIBIT 9 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE OF PAGES

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. It was the regular practice of the business activity to make the records; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

DCGS-A_V3.1_P3_BAL_VDD_149015_Rev1_1_Oct_09.doc (14 pages)

-Nothing Follows--

Organization

S FAE -IEW- DCG - PM DCGS -A

Signature	Date
florinda white	4/11/2012
Print or Type Name	Title
FLORINDA WHITE	PM DCGSA configuration MGR
Business Telephone	Business Address
(443) 867-3783	BLDG 6006 Combat Drive Aberdeen Proving Ground, MD 21005

Subscribed and sworn to before a notary public, this 1st day of April, 2012.

Notary Public	My commission expires on: MINDY K. DECKER NOTARY PUBLIC OF NEW JERSEY Commission Expires 11/19/2013
---------------	--

UNCLASSIFIED//FOUO

**Version Description Document (VDD)
For**

**Basic Analyst Laptop
(BAL)**

**Distributed Common Ground Systems – Army
Software Version 3.1 Patch 3
(DCGS-A V3.1 P3)**

1 October 2009



DCN: 149015, Rev 1

UNCLASSIFIED//FOUO

Revision History

Revision	Date	Page(s)	Para.	Description of Change
Original	February 17, 2009	N/A	N/A	Initial release
1	October 1, 2009	N/A	N/A	Release of new Image with Re partition of Drives, with SQL, Data Base hardening and configuration changes

1.	Scope	1
1.1	Identification	1
1.2	System Overview.....	1
1.3	Document Overview.....	1
2.	Referenced Documents.....	1
3.	Version Description	1
3.1	Inventory of Materials Released	1
3.2	BAL Media Listing.....	2
3.3	Software Description	2
3.4	Possible Problems and Known Errors.....	6
3.5	Adaptation data	7
3.6	Related Documents	7
3.6.1	Post Clone Procedures	7
3.6.2	Installation Procedures.....	7
3.6.3	Technical Bulletins	7
3.6.4	Overwatch MFWS Release 6.2.....	9
3.7	COTS Software Sites	10
3.8	Hardware Description.....	10

1. Scope

1.1 Identification

This Version Description Document (VDD) describes software release V3.1 P3 being developed at the direction of the Project Manager DCGS-A for use in the DCGS-A V3.1 P3 Basic Analyst Laptops (BALs), which include Dell M90, M6300, and the Alienware (A51M). Two other Client platforms are the Dell M490 Workstation, T5400 Desktop. The BALs, Workstation and Desktop software version will be authorized to process up to Secret Collateral information and connect to the Secret Internet Protocol Router Network (SIPRNET) in accordance with AR 25-2 Information Assurance and Department of Defense (DoD) Instruction 8500.2 Information Assurance (IA) Implementation.

1.2 System Overview

The A51M, M90 and/or M6300 are high-end laptop computers with a 17" monitor capable of displaying high-resolution graphics. The Dell 490 Workstation and T5400 Desktop with the V3.1P3 SW is used within the DCGS-A fixed site baseline. Microsoft Windows XP Professional (Service Pack3) utilized as the operating system. The A51M, M90, M6300, Dell 490 and T5400 provide the Army a client workstation for use by DCGS-A analysts.

Note: The A51M, M90, M6300, Dell 490 and T5400 is classified because of a file change within the Query Tree Multi Functional Work Station (MFWS) Plug-In and the change to the high water marking.

1.3 Document Overview

This VDD documents the release tested and type-accredited with the DCGS-A V3.1 P3 Collateral components in the DCGS-A laboratory environment at Fort Monmouth, NJ, released to the Central Technical Support Facility (CTSF), Fort Hood, TX; and then released to operational users for site accreditation.

2. Referenced Documents

Field Service Engineer (FSE) Training Guide, Part # 3.1.03.1002.C, dated 1 October 2009 prepared by I2WD, Fort Monmouth NJ.

Note: All referenced documents are resident in the Software Engineering Center (SEC) Software Control and Reference Office (SCRO).

3. Version Description

3.1 Inventory of Materials Released

Software for the DCGS-A V3.1 P3 BAL is installed at the Software Integration Lab (SIL) onto the laptop's hard drive. Consequently, no media will be delivered with the DCGS-A V3.1 P3 BAL. All updates are provided through download from digital media.

25 Hard Drives and 3 DVDs containing software and documentation for DCGS-A Version 3.1 P3 is resident in the Software Engineering Center (SEC) Software Control and Reference Office (SCRO) reference on paragraph 3.2. BAL Media Listing.

3.2 BAL Media Listing

CM Control Number	SCRO CINCODE	Date of media	Destination	Created By	Contents	Media Type
DCGS0303	N/A	4-Nov-09	SEC IFS/ SCRO	SEC SCIF	DCGS-A V3.1P3 - M90 and/or M6300; Alienware (A51M); Dell 490 Workstation and T5400 Desktop Client Image - Secret	1 HD
DCGS0318	N/A	1-Oct-09	SEC IFS/ SCRO	SEC SCIF	DCGS-A V3.1 P3 – APP1, APP2, IOP, MDC & BALs Image	1 set of 1 HD

3.3 Software Description

The following is a list of DCGS-A V3.1 P3 Client SW detailed software information:

NOTE: The Client SW listed can be loaded on the five platforms that include Dell M90, M6300, A51M, Dell M490 Workstation and the Dell T5400 Desktop. Once the SW is loaded onto the platform, the appropriate drives are loaded. The I2 Analysis Notebook (ANB) is loaded on the system without an active software license, if the user chooses to use ANB; the user will procure the license. The Axis Pro capabilities are in the DCGS-A MFWS V3.1.

BAL Software	Version	Vendor	Function/Component
Acrobat Reader 9	9.1.2	Adobe	PDF file reader
Adobe Flash Player Plug-in	10.0.32.18	Adobe	Adobe Flash is the authoring environment and Flash Player is the virtual machine used to run the Flash files
Adobe Flash Player 10 Active X	10.0.22.87	Adobe	Flash Player
Alert Services Client Runtime (ALTCLT)	4.53.5	Future Skies	Alert Service Application
ArcGIS Desktop	9.2.1500	ESRI	Geospatial data management and presentation
ArcMap	9.2	ESRI	Geospatial data management and presentation
ArcGIS Military Analyst (Military Analyst 9.2 SP2)	9.2.401	ESRI	Geospatial data management and presentation
ArcGIS Military Overlay Editor 9.2 (SP1)	9.2.0.430	ESRI	Geospatial data management and presentation
CECOM_MapShapes	1.00.0000	Overwatch	
Chart Scrapper	7.2.0.1	Novel Application	Data Movement tool

BAL Software	Version	Vendor	Function/Component
C2R	4.70.9	GOTS/PD CS	Address Book Services
C2R Planner	1.00.0000	GOTS/PD CS	Address Book Services
CMP	4.7.0.6	GOTS/PD CS	Common Message Processor
DB Importer	7.1.0	Novel App Inc.	DB Importer
DCGS-A Configuration Assistant	1.3.0 20090504	I2WD	Post clone assistant
DCGS-A MFWS V3.1	6.2.6.1077	Overwatch	Multi function Workstation DCGS-A APP Framework SDK; v 1.7.13
DCGS-A_V3.1_Full	6.2.0.1035	Overwatch	Multi function Workstation
DCGS-A Multimedia Plugin	1.0.0	BAH	Multi function Workstation
DCGS-A Web Folder Plugin	2.0.0	BAH	Multi function Workstation
DjCI (DOS Client Interface)	5.1.5.0	Future Skies	
DCGS-A Weather IWEDA Client Tri-Service IWEDA -20061129	6.4.2.8	Army Research Lab	Weather effect decision aid
Digital Topographic Support Systems (DTSS) 9.0 6 Rendering Package	9.0	Northrop Grumman	To provide critical, timely, and accurate digital and hardcopy geospatial information
DIB Client Adapter	1.3	CSP Tech	Installer for the Viper DIB Client Adapter
GeoRover for ArcGIS	3.10.0000	SAIC	Geospatial software product extensions or "plugins" to ArcMap
GeoRover Coordinate Viewer Extension	1.0.2	SAIC	Geospatial
GeoRover Digital Data Tracker Extension	3.2.5	SAIC	Geospatial
GeoRover License Manager	1.1.0	SAIC	Geospatial
GeoRover Locus Track Extension	3.2.4	SAIC	Geospatial
GeoRover Zoom Tools Extension	3.2.4	SAIC	Geospatial
Ground Tactical Communication (GTCS)	4.7.0.9	GOTS/PD CS	Message Transport Protocol

BAL Software	Version	Vendor	Function/Component
Google Earth EC	4.2.205.5730	Google	Virtual globe, map and geographic information
Grid Extractor	1.2		
i2 Analyst Notebook 6	6.055.1022	i2	Link & Timeline Analysis tool w/ graphical representation
i2 Online Link 6	6	i2	i2 Online iLink is a feature of Analyst's Notebook 6 that optimizes online data research and analysis. It enables real-time access to online data providers.
i2 Chart Reader 6	6	i2	Charts Reader
i2 Chart Reader 7	7.0.7	i2	Charts Reader
i2 Image Files	6	i2	Image Editors
i2 Visual Notebook	6	i2	Visualization software, streamlines investigations
i2 Spelling Checker	6	i2	Image Editors
IIS URL Scan Tool	2.0		
IME Pass Client			
IME WWF Client			
JAVA™ 6 Update	1.6.0.60	Sun Micro	Program language compiler and environment
Live Update 3.2	3.2.0.68	Symantec	Software Update Tool
Microsoft .NET Framework 3.0 SP1	3.1.21022	Microsoft	Environment for building, deploying, and running web services and other applications
Microsoft .NET Framework 2.0 SP1	2.121022	Microsoft	Environment for building, deploying, and running web services and other applications
Microsoft .NET Framework 1.1	1.1.4322	Microsoft	Environment for building, deploying, and running web services and other applications
Microsoft Compressive Client1.0 for Window XP	1.0	Microsoft	
Microsoft Office Professional Plus Edition 2007	12.0.6215.1000	Microsoft	Electronic office tools
Microsoft Office 2003 Web components	11.0.6558.0	Microsoft	Allows embedding and linking to documents
Microsoft Office XP Web components	10.0.6619.0	Microsoft	Allows embedding and linking to documents

BAL Software	Version	Vendor	Function/Component
Mozilla Firefox	3.0.5	Mozilla	Web Browser
MS SQL Server 2005	9.2.3042.00	Microsoft	Database
MS SQL Server 2005 Backward Compatibility	8.05.2004	Microsoft	Database
MS SQL Server 2005 Books On-Line (English)	9.00.1399.06	Microsoft	Database
MS SQL Server Native Client	9.00.3042.00	Microsoft	Database
MS SQL Server Setup Support Files	9.00.4035.00	Microsoft	Database
MS SQL Server VSS Writer	9.00.4035.00	Microsoft	Database
MS User Mode Driver Framework Feature Pack 1.0	1.0	Microsoft	Build #5716
MSXML 6.0 Parser	6.10.1129.0	Microsoft	Text parser
MSXML 4 SP2	4.20.9818.0	Microsoft	Text parser
MSXML 4 SP2	4.20.9870.0	Microsoft	Text parser
MSXML 4 SP2	4.20.9848.0	Microsoft	Text parser
02 Micro Smartcard Driver	2.26.0000	02 Micro Electronics, Inc.	
OZ776 SCR CardBus	1.1.4.2	02 Micro Electronics, Inc.	
Psi	.12	GNU	Collaboration Tool
Python	2.4.1	Open Source	Object Oriented programming language
QuickTime	7.64.17.73	Apple	Audio and video file player
Query Tree MFWS Plugin	1.3.8	I2WD	MFWS Plugin
Roxio Activation Module	1.0	Roxio	Digital Media Software
Roxio Creator Audio	3.5.0	Roxio	Digital Media Software

BAL Software	Version	Vendor	Function/Component
Roxio Creator Copy	3.5.0	Roxio	Digital Media Software
Roxio Creator Data	3.5.0	Roxio	Digital Media Software
Roxio Creator DE	3.5.0	Roxio	Digital Media Software
Roxio Creator Tools	3.5.0	Roxio	Digital Media Software
Roxio Drag-to-Disc	9.1	Roxio	Digital Media Software
Roxio Express Labeler 3	3.2.1	Roxio	Digital Media Software
Roxio Update Manager	6.0.0	Roxio	Digital Media Software
Shared Add-in Extensibility update for MS .Net Framework 2.0	1.0.0	Microsoft	
Shared Add-in Support Update for MS .Net Framework 2.0	1.0.0	Microsoft	
Sigma Tel Audio	5.10.5210.0	SigmaTel	Digital audio processing
Smart Link 56k Voice modem			Voice modem
Sonic Cine Player Decoder Pack	4.2.0	Sonic Solutions	
Symantec AntiVirus	10.1.8000.8	Symantec	Virus detection
SQLXML 4	9.00.4035.00	Microsoft	
Synaptics Pointing Device	7.13.2.0	Synaptics	Pointing device
Threat Mapper 1.1 for ArcGIS Desktop	1.1		
Windows Internet Explorer 7 - 20070813.185237	7.0.5730.13	Microsoft	Web Browser
Windows Media Player 11	11.0	Microsoft	Media Player CD, DVD, streaming audio & video
Windows Media Format 11 Runtime	11.0	Microsoft	Media Player
Windows XP SP3	2008.0414.03 1535	Microsoft	
WinZip	10.0 (6685)	Winzip Computing LP	File compression
Xalan – Endorsed	1.00.0000	Overwatch	XML processing package

3.4 Possible Problems and Known Errors

See ReadMe document for DCGS-A V3.1.0P3 Multi-Function Work Station (MFWS) and Interoperability (IOP) Server, dated 17 February 2009, I2WD SIL.

3.5 Adaptation data

Not applicable

3.6 Related Documents

3.6.1 Post Clone Procedures

Refer FSE Training Guide in Section 2, Referenced Documents

3.6.2 Installation Procedures

DCGS-A V3.1.0P3 Multi-Function Work Station (MFWS) and Interoperability (IOP) Server ReadMe.doc, dated 17 February 2009, I2WD SIL

DCGS-A V3.1P3, Update Image Restore ReadMe.doc, dated 1 October 2009, I2WD SIL

3.6.3 Technical Bulletins

TB-DCGS 09-10087 – re: Workstation vulnerabilities fixes, 17 February 2009

TB-DCGS 09-10097 – re: DISA Gold/POA&M data, 17 February 2009

NOTE: TB-DCGS 09-10087 and TB-DCGS 09-10097 were implemented in the software baseline delivered to CTSF on 17 February 2009, and are under Application 2 server.

The following Technical Bulletins applies to the V3.1P3 SW baseline after 17 February 2009 delivery to CTSF:

TB Number	Configuration Systems	Title/Topic	PM DCGS-A Approved
DCGS 09-10094	MDC	Undeployment of DIB brain Adapter and /or PW update to xpipeline account; also adds DIB and portal versioning	11-May-09
DCGS 09-10095	IOP	IOP office 2007	11-May-09
DCGS 09-10099	MSMQ service on BALs	Fixes problem sending USMTF and PASS messages from BAL in standalone mode. (4 March 2009)	14-May-09
DCGS 09-10100	APP1	Fixes APP1 homepage / baseline map problems (6 March 2009)	11-May-09
DCGS 09-10101	APP1	Fixes publishing Graphics to DIB problem (4 March 2009)	11-May-09
DCGS 09-10104	BAL	Adds Ft. Hood Maps to BAL (23 March 2009)	7-May-09
DCGS 09-10106	BAL	Fixes problem with SWB1 IWEDA Client (31 March 2009)	11-May-09
DCGS 09-10107A	BAL & IOP	QT plugin ver1.3.8.1 update - allows working with BOTH OIF and OEF data (09 April 2009)	12-May-09
DCGS 09-10108	MDC	Adds Ft. Huachuca Mini brain link to MDC portal (17 April 2009)	11-May-09
DCGS 09-10111	IOP	Fixes problem clearing the TED DB after a training event (20 April 2009)	7-May-09
DCGS 09-10112A	APP1, APP2, MDC, IOP, BAL	Configuration Assistant Update to v1.3.0 (5 May 09)	14-May-09
DCGS 09-10113	APP1	NAI fix for Firefox	11-May-09

TB Number	Configuration Systems	Title/Topic	PM DCGS-A Approved
DCGS 09-10115A	BAL	Fix for sending TED entities to Google Earth	18-May-09
DCGS 09-10116	BAL	Changing permission settings for DCGS-A User folder	7-May-09
DCGS 09-10120	MFWS	Allow the operator to enter a full non-western name in QuickForms and/or the Properties plugin without incorrectly mapping them to middle and last name fields	28-May-09
DCGS 09-10122	IOP, BAL	Applies to all v3.1 P3 DCGS-A DCGS IOP servers and BALs systems. It edits registry values to allow for the workflow between Google Earth and MFWS to be successful	3-Jun-09
DCGS 09-10123	BAL	Provides corrections to the DIB plug-in of the BAL MFWS. The TB corrects issues with the DIB usage found in the SIL Bug Tracker	15-Jun-09
DCGS 09-10126	IOP, BAL	Server Vulnerability Fixes. Hides DIB & Query Tree data drivers from the users display within Google Earth	3-Aug-09
DCGS 09-10128	APP2	Server Vulnerability Fixes. Users are unable to convert ANB7 charts to ANB6 charts	21-Aug-09
DCGS 09-10129		Python 2.4 win32 extensions install	3-Aug-09
DCGS 09-10131B	MSG, SDE	Server Vulnerability Fixes (LiSTA 0.7.5) for P3 & P5 systems (Red Hat 5 / 32 BIT)	21-Aug-09
DCGS 09-10132	BAL	Add mlRC chat to BAL baseline	24-Aug-09
DCGS 09-10133	BAL	Add correct ESRI Arc Desktop 9.2 License to Baseline for use of Tracking Analyst	2-Sep-09
DCGS 09-10134	BAL	Firefox Flash installation	2-Sep-09
DCGS 09-10137A	APP1	JBOSS windows service fix	10-Sep-09
DCGS 09-10147	APP1, APP2, MDC, IOP, BAL	Microsoft Windows Server / Workstation Vulnerability Fixes - SAT v1.2.1b	23-Sep-09
DCGS 09-10148	BAL, IOP	MFWS Merge Relationships, Deleted Entity Manager Updates	9-Oct-09
DCGS 09-10149A	MDC	JBOSS windows service fix (startJBoss.cmd / wrapper.dll)	27-Oct-09
DCGS 09-10152	BAL, IOP	Removal of duplicate IIS Web folders from C:\DCGS directory	16-Oct-09
DCGS 09-10153	BAL, IOP	Issues Discovered in OIF and OEF_17 Feb 09 Image	23-Oct-09
DCGS 09-10155	MSG, SDE	Server Vulnerability Fixes - LiSTA v0.7.7 (RHEL5 / 32 BIT) i386	27-Oct-09
DCGS 09-10157	APP1, APP2, IOP, MDC, BAL	Microsoft Windows Server / Workstation Vulnerability Fixes - SAT v1.2.1	3-Nov-09
DCGS 09-10159	BAL, IOP	Issues discovered in OIF and OEF (OW_P7) This TB supersedes TB 10153	6-Nov-09

3.6.4 Overwatch MFWS Release 6.2

DCGS-A V3.1, MFWS release 6.2, Document number: 102168, dated 15 January 2009, Overwatch
Textron Systems

3.7 COTS Software Sites

- 3D analyst (ArcGlobe)
 - <http://www.esri.com/software/arcgis/extensions/3danalyst/index.html>
- Acrobat Reader
 - <http://www.adobe.com>
 - <http://www.esrl.com>
- Analyst Notebook
 - <http://www.i2.co.uk>
- Java
 - <http://java.sun.com/>
- Microsoft
 - <http://www.microsoft.com/>
- Netscape
 - <http://www.netscape.com/>
- Roxio
 - <http://roxio.com>
- Symantec
 - <http://www.symantec.com/index.htm>
- Winzip
 - <http://www.winzip.com/>
- WS_FTP
 - <http://www.ipswitch.com/>

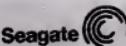
3.8 Hardware Description

The following is a list of DCGS-A V3.1 P3 BALs hardware information:

Component	Description
Alienware Laptop - Model A51M	3.8 GHz, 2GB RAM memory, 17" display with high resolution graphics.
Dell Laptop - Model M90	2.33 GHz Intel Dual Processor Core, 3.25GB RAM memory, 93.1 GB hard drive, with NVIDIA graphics card, DCD-RW Optical Drive, Network Interface Card and a 17 inch display with high resolution graphics.
Laptop - Model Dell M6300	2.5 GHz Intel Core 2 Duo T9300, 4GB DDR2-667 SDRAM (2 DIMM), NVIDIA Quadro FX3600M 512 MB, 160 GB 7200RPM Hard Drive, Std Touchpad, 8x DVD+/- & Roxio Creator , and a 17" wide screen WUXGA LCD.
Dell Precision 490 Workstation	1st Processor: Intel XEON DUAL CORE Processor 3.00GHZ, 2MB L2 Cache; 2nd Processor: Intel XEON DUAL CORE Processor 2.80GHZ, 2MB L2 Cache; 4GB, DDR2 ECC SDRAM Memory, 400MHZ; NVIDIA FX 4500 512MB 2 DUI OR GA 1st Hard Drive: 80GB Serial ATA 7200RPM Hard Drive w/Databurst Cache, Non-Raid, Precision 470/670; 2nd Hard Drive: 80GB Serial ATA 7200RPM Hard Drive with

Component	Description
	Databurst Cache Raid; Floppy Drive: 3.5, 1.44MB; 48X/32X CD-RW/DVD Combo.
Dell Precision T5400 Desk Top	1st Processor: Quad Core Xeon Proc X5450, 3.00GHz, 2X 6MB L2 Cache,1333MHz; 2nd Processor: Quad Core Xeon Proc X5450, 3.00GHz, 2X6MB L2 Cache,1333MHz, 4GB, DDR2 ECC SDRAM Memory 667MHz, 4X1GB; NVIDIA Quadro FX3700 512MB dual DVI Graphics Card; 160GB SATA, 10K RPM Hard Drive with 16MB DataBurst Cache; CD-ROM or DVD-ROM Drive: 16X DVD+/-RW.

PROSECUTION EXHIBIT 11 for identification
PAGE OFFERED _____
PAGE ADMITTED _____
PAGE ____ OF ____ PAGES



S/N: 8V625GSM

ST31500341AS

P/N: 8JU138-302

Firmware: CC1H

Date Code: 09502 Site Code: TK

Barracuda 7200.11
1500 Gbytes

+ 5V 0.72A
+ 12V 0.52A

Product of Thailand

Caution. Product warranty is void if any seal or label is removed, or if the drive experiences shock in excess of 350 Gs.

STX-720011 (B)

Need Support? Visit www.Seagate.com.

Installation Summary

For easy installation use Seagate's DiscWizard™ software, available at www.seagate.com/support. Always backup critical data before making changes.

Serial ATA controllers and system BIOS have several setup choices. See your controller or system documentation for specific options and any custom device drivers.

1. Mount the drive using four screws per side. Do not over tighten the screws.

2. Attach the cables. The data interface and power cables are keyed.

3. Turn your computer. Run the system setup program. Enable the new drive and set the options.

4. Prepare the drive for use with your Operating System. See your OS Help instructions for details.

Be careful to select the correct drive. Windows® Vista or XP prepares the drive during installation.

If this is a second partition, Windows Disk Management can be used to prepare the drive.

Use the DiscWizard software to copy data from an old drive to a new drive.

Go to www.seagate.com/support and select Installation for additional instructions and illustration.

Macintosh and Slim USB key in the utilities folder.

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 7071-1
(48)

This medium is

UNCLASSIFIED

Substitute for
Prosecution Exhibit 11

PROSECUTION EXHIBIT 12 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE OF PAGES

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

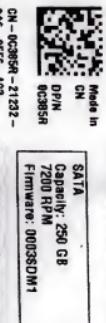
This medium is

UNCLASSIFIED

U.S. Government Property

SE 710 (1-87)

卷之三



Momentum 7200
250 Gi
Canada Class B digital apparatus ICES-003

Momentum 7200

Seagate

**Substitute for
Prosecution Exhibit 12**

EVIDENCE/PROPERTY TAG

For use of this form, see AR 35-5,
the proponent agency is DCS, G-3

DOCUMENT NUMBER

010-10

MPR/CID CONTROL NUMBER

0028-10-CI0221-10117

ITEM NUMBER

1 OF 1 ITEM

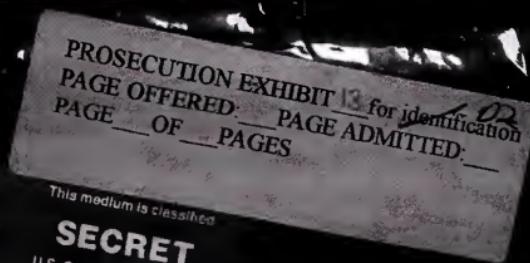
TIME DATE INITIALS
0100 12 Jun 10 APC

REMARKS

Mr. Adrian A. Lamo's
Hard Disk Drive
Serial Number
K404F812mf4D

DA FORM 4002, JUL 92

Replaces DA Form 4002, 1 JUL 76 which is obsolete.



This medium is

UNCLASSIFIED

U.S. Government Property

SF 710 (4-87)

HOS001B

SF>

**Substitute for
Prosecution Exhibit 13**

PROSECUTION EXHIBIT 4 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE 02 OF PAGES

EVIDENCE/PROPERTY TAG		
For use of this form, see AR 195-5. the proponent agency is DCS, G-3		
DOCUMENT NUMBER	077-10	
MPR/CID CONTROL NUMBER 0028-10-CID 221-10117		
ITEM NUMBER	OF	ITEM
TIME	DATE	INITIALS
0208	12 Jun 10	APF
REMARKS MR. Adrián A. Lamo's Laptop Computer APM mini brand w/ power supply		

DA FORM 4002, JUL 92

Replaces DA Form 4002, 1 JUL 78, which is obsolete.

This medium is

UNCLASSIFIED

Substitution for
Prosecution Exhibit 14

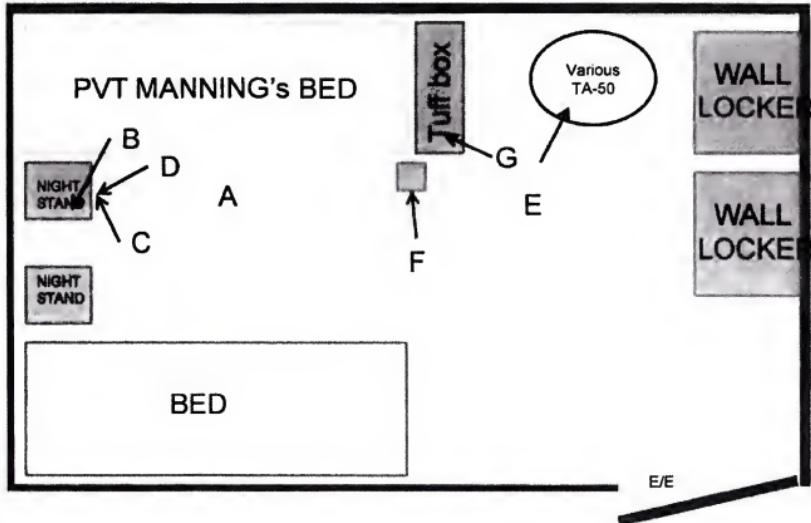
Prosecution Exhibit 15
has been entered into
the record as a CD/DVD
and will be maintained
with the original
Record of Trial



ManningB_00527547

PROSECUTION EXHIBIT 15 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE ____ OF ____ PAGES

Rough Sketch Depicting PFC MANNING's ROOM



LEGEND

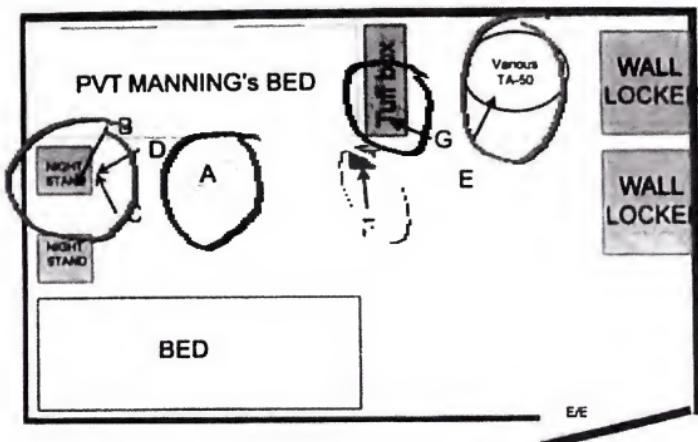
- A: Apple laptop computer on computer stand
- B: Two writable CDs found on nightstand
- C: Cellular Telephone in nightstand drawer
- D: Eight DVDs found in nightstand cubby
- E: External Hard drive in assault pack
- F: CD in box
- G: Camera on tuff box

N
↑
NOT TO SCALE

TITLE BLOCK

CASE NUMBER: 0160-10-CID899-14463
OFFENSE: Disclosure of Classified Information
SCENE PORTRAYED: Room 14B, Brigade Headquarters
LOCATION: FOB Hammer, Iraq
VICTIM: US Government
SUBJECT: PFC MANNING
TIME/DATE BEGAN: 0030/28 May 10
SKETCHED BY: SA Thomas A. SMITH
VERIFIED BY: SA Toni M. GRAHAM

For Official Use Only Law Enforcement Sensitive

0028-10-CID221-10117
0160-10-CID089-14463**Rough Sketch Depicting PFC MANNING's ROOM****LEGEND**

- A Apple laptop computer on computer stand
- B Two writable CDs found on nightstand
- C Cellular Telephone in nightstand drawer
- D Eight DVDs found in nightstand cubby
- E External Hard drive in assault pack
- F CD in box
- G Cameras on tuff box

NOT TO SCALE

TITLE BLOCK

CASE NUMBER: 0160-10-CID089-14463
 OFFENSE: Disclosure of Classified Information
 SCENE PORTRAYED: Room 148 Brigade Headquarters
 LOCATION: FOB Hammer, Iraq
 VICTIM: US Government
 SUBJECT: PFC MANNING
 TIME/DATE BEGAN: 0030/28 May 10
 SKETCHED BY: SA Thomas A. SMITH
 VERIFIED BY: SA Toni M. GRAHAM

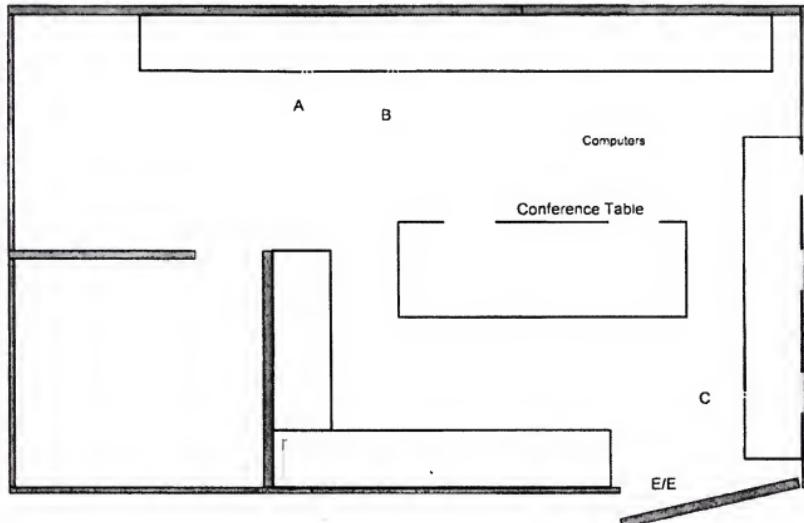
For Official Use Only Law Enforcement Sensitive

ManningB 00000285

16

Exhibit 26
Identification
02PFC MANNING
FBI - TAMPA
MAIL CENTER
PO BOX 10000

Rough Sketch Depicting Crime Scene



LEGEND

- A. Location of SIPR Computer
- B. Location of SIPR Computer
- C. Location of NIPR Computer

↑

N

NOT TO SCALE

TITLE BLOCK

CASE NUMBER: 0160-10-CID899-14463
OFFENSE: Disclosure of Classified Information
SCENE PORTRAYED: Room 14B, Brigade Headquarters
LOCATION: FOB Hammer, Iraq
VICTIM: US Government
SUBJECT: PFC MANNING
TIME/DATE BEGAN: 2330/27 May 10
SKETCHED BY: SA Thomas A. SMITH
VERIFIED BY: SA Toni M. GRAHAM

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT

PROSECUTION EXHIBIT 17 for identification
PAGE OFFERED _____ ADMITTED _____
PAGE ____ OF ____ PAGES

PROSECUTION EXHIBIT 18 for IDENTIFICATION
PAGE OFFERED: 1 PAGE ADMITTED: 1
PAGE 1 OF 1 PAGES

ManningB_00000344

ManningB 00000344



PROSECUTOR EX H 18a *02* w identification
PAGE 1 OF 1 ADMITTED:
PAGE 1 OF 1 PAGES

2013-06-03 14:58:43

ManningB 00000344



PROSECUTION EXHIBIT 18b for identification
PAGE OFFERED: PAGE ADMITTED: 12
PAGE OF PAGES

2013-06-03 15:02:13

R
PROSECUTION EXHIBIT 19 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE _____ OF _____ PAGES

ManningB_00000302



ManningB 00000302

PROSECUTION EVIDENCE 19a for identification
PAGE 1 OF 1 TOTAL PAGE 1 OF 1

PROSECUTION EXHIBIT 20 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE ____ OF ____ PAGES

ManningB_00000304

ManningB 00000304



PROSECUTION EXHIBIT 20 for identification
PAGE OFFERED: _____ GE ADMITTED: _____
PAGE 02 OF 1 PAGES

2013-06-03 14:41:17

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)
)
)
)

STIPULATION OF
EXPECTED TESTIMONY

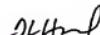
SGT Mary Amiatu

DATED: 30 May 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if SGT Mary Amiatu were present to testify during the merits and pre-sentencing phases of this court-martial, she would testify substantially as follows.

1. I am currently the S-1 NCO for the 6th Engineer Battalion at Fort Richardson, Alaska. I have held this position for two months. Previously, I was the Strength Accounting Clerk for U.S. Army Central Command G-1 at Camp Arifjan, Kuwait. I held that position from October of 2011 until October of 2012. In that position, I helped account for personnel coming in and out of theater, moving from place to place within theater, and changing duty status. I provided battle management update briefs and worked with the Deployed Theater Accounting System (DTAS). I also worked with the Joint Asset Movement Management System (JAMMS).
2. With regard to this particular investigation, I provided investigators from the Army Criminal Investigation Command (CID) a print-out from JAMMS on PFC Bradley Manning. JAMMS is a system that captures movement and location information about operating forces, government civil servants, and government contractors through data collection points established in specified operational theaters. These collection points are, for example, dining facilities, ports of debarkation, and fuel points. Operational theaters include Kuwait, Afghanistan, and Iraq. As such, JAMMS would capture the dates on which PFC Manning scanned himself in and out of Department of Defense (DOD) facilities using his CAC card, such as dining facilities (DFACs) and points of debarkation into and out of Iraq (APOD/SPOD). When providing this report, I also signed and had notarized an attestation certificate (identified at BATES Number 00412522) regarding the authenticity of the information.
3. As a former Strength Accounting Clerk, I am familiar with JAMMS reports. I have read them before. I, therefore, understand this JAMMS report I provided (identified at BATES Numbers 00412523 - 00412532) to show that the Service Member named "Manning, Bradley", whose last four social security number digits are , came into and out of Iraq several times. For example, on page 9 of this document, it shows that on 26 October 2010, PFC Manning signed into the DFAC on Camp Buehring in Kuwait, but by 28 October 2010, was using the DFAC in Iraq. Page 8 shows Bradley Manning departed Iraq on 22 January 2010 and then entered again, via Kuwait, on 11 February 2010. Gaps like this are normal when a soldier leaves a deployed environment, such as for mid-tour leave. Page 8 further shows that PFC Manning was using the FOB Hammer DFAC by 14 February 2010. Lastly, Page 1 shows that PFC Manning boarded an outbound flight from Iraq on 30 May 2010.


ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel


THOMAS F. HURLEY
MAJ, JA
Defense Counsel


BRADLEY E. MANNING
PFC, USA
Accused

ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

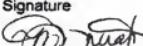
1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrences of the matters set forth by or from information transmitted by, people with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. It was the regular practice of the business activity to make the records; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

* JOINT ASSET MOVEMENT MANAGEMENT SYSTEM
PERTAINING TO PFC BRADLEY MANNING AS OF
15 FEB 12.

Organization

US ARMY G1 SAMB SECTION, CHINP ARIF JAN KU, AFSC AE 0930G

Signature	Date
	15 FEB 12
Print or Type Name	Title
MARY HOWELL	SAMB CLERK
Business Telephone	Business Address
430-6314 (DSN)	AFSC AE 0930G (CFC)



The attached record consists of _____ pages (1 files).

Subscribed and sworn to before a notary public, this 15 day of February, 20 12.

Notary Public	My commission expires on:
Yeon A. Howell, SGT LEAH A. HOWELL	TITLE 10 USC 1044A

PROSECUTION EXHIBIT 22 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE 1 OF 1 PAGES

FOR OFFICIAL USE ONLY

JAMMS Movement Report by Person

Generated as of Feb 15 2012 12:15 GMT

Total records returned: 204

Full Name	Foreign National Status	Last 4 digits of SSN or FIN	Personnel Category	Person Is In SPOT (Y/N)?	Scan Date	Country	Scan Location Type	Scan Location Name	Movement Direction
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/30/2010	Iraq	APOD	LIBERTY PAD (OUTBOUND) BIAP	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/29/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/28/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/28/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/28/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/28/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/27/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/26/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/26/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/25/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/24/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/21/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/19/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/19/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/18/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/18/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen		U.S. Military Personnel	N	5/17/2010	Iraq	DFAC	Camp Hammer	Arrival

PRINT DATE: 2/15/2012

Page 1 of 10

Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	5/2/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	5/1/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	5/1/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/30/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/29/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/27/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/27/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/26/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/26/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/25/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/25/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/24/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/24/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/23/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/22/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/22/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/22/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/22/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/21/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/21/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/21/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/21/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	4/20/2010	Iraq	DFAC	Camp Hammer	Arrival

PRINT DATE: 2/15/2012

Page 3 of 10

Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/23/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/23/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/23/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/22/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/22/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/20/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/20/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/19/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/19/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/19/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/18/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/18/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/18/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/17/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/16/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/16/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/16/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/15/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/14/2010	Iraq	DFAC	Camp Hammer	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/12/2010	Iraq	DFAC	Hard Rock(Camp Stryker)	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/11/2010	Iraq	APOD	BIAP HELO	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	2/11/2010	Kuwait	APOD	Kuwait APOD/SPOD Tent 3, Outbound	Departure
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	1/22/2010	Iraq	APOD	BIAP HELO	Departure

Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	1/22/2010	Iraq	DFAC	Air Power (Sather AB)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	1/22/2010	Iraq	DFAC	Air Power (Sather AB)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	1/21/2010	Iraq	APOD	BIAP HELO	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	1/21/2010	Iraq	DFAC	Hard Rock(Camp Stryker)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/28/2009	Iraq	APOD	BIAP HELO	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/28/2009	Iraq	DFAC	Air Power (Sather AB)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/28/2009	Iraq	APOD	BIAP HELO	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/26/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/25/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/24/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/24/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/24/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/21/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/21/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/21/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/19/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/18/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/18/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/18/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/17/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/17/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/16/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	U.S. Military Personnel	N	10/16/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival

Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	10/14/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	10/13/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	10/13/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival
Manning, Bradley	U.S. Citizen	[REDACTED]	U.S. Military Personnel	N	10/12/2009	Kuwait	DFAC	CAMP BUEHRING (AIK)	Arrival

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)
)
)
)

STIPULATION OF
EXPECTED TESTIMONY

SA Calder Robertson

DATED: 3 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent Calder Robertson were present to testify during the merits and pre-sentencing phases of this court martial, he would testify substantially as follows:

1. I am a Special Agent (SA) for the Computer Crime Investigative Unit (CCIU) of the U.S. Army Criminal Investigation Command (CID). I have been with CCIU since March 2006. In February 2010, I became the Special Agent-in-Charge (SAC) of the Europe Branch Office of CCIU. In my current capacity, I am responsible for conducting and overseeing the conduct of large-scale complex criminal investigations associated with high technology, including insider threat and computer intrusions into the critical information architecture of the U.S. Army. Among other things, this work includes: conducting interviews, executing search warrants, processing crime scenes, collecting and handling physical evidence, obtaining forensic images of digital evidence, conducting forensic examinations, and preparing comprehensive reports for supported officials and prosecutors. I have testified several times in judicial proceedings. Because I am in charge of the Europe Branch Office of CCIU, I have responsibility for investigating cyber crime incidents in Europe and Africa, as well as providing rapid response to Southwest Asia (Iraq and Afghanistan). Additionally, I was recently selected to establish the Pacific Branch Office of CCIU, with responsibility for investigating U.S. Army cyber crime incidents in the Pacific area of operations. From April 1998 to November 2003, I held a variety of other positions within CID and was responsible for investigating criminal offenses with an Army nexus.
2. I received a B.S. in Psychology in 2006 and have been a Certified Computer Crime Investigator through the Defense Cyber Crime Center (DC3) since 2007. In 2010, I was awarded the U.S. Army Achievement Medal for Distinguished Civilian Service as a civilian Special Agent for Army CID. I have received numerous other awards in my civilian and military capacities.
3. I have received extensive training from the Defense Cyber Investigations Training Academy (DCITA), which is part of DC3. Through DCITA, I have attended the following courses relevant to my current work: Live Network Investigations (2009), Mobile Electronics Forensics Training (2008), Advanced Log Analysis (2008), Forensics and Intrusions in a Windows Environment (2007), Macintosh Forensic Examinations (2007), Wireless Technology (2007), Windows Forensic Examinations with EnCase (2007), Introduction to Networks and Computer Hardware (2006), and Introduction to Computer Search and Seizure (1999). Additionally, I attended Computer Forensics II with EnCase in 2009, a course put on by Guidance Software, the

makers of EnCase. In 2011, I also attended DCITA's Large Data Set Acquisition course as well as the Army Criminal Investigation Laboratory's Evidence Management Certification Course. These courses focused on the collection and handling of physical and digital evidence.

4. On 27 May 2010, I became involved with the investigation of PFC Bradley Manning after receiving preliminary information on misconduct that required downrange investigation. As the SAC of the Europe Branch Office of CCIU and the closest CCIU agent to Iraq, I was tasked by CCIU Headquarters, then at Fort Belvoir, Virginia, to provide support to the Camp Liberty CID office. I traveled to Camp Liberty in Baghdad and stayed there for three days at the end of May 2010. I stayed at Camp Liberty because, at that time, it was too dangerous to travel to FOB Hammer. Additionally, the evidence collection team already at the crime scene on FOB Hammer had sufficient personnel to complete their mission such that my physical presence was unnecessary. My role in the investigation was to assess and provide expert assistance with the collection, preservation, and imaging of computer evidence as well as to perform preliminary analysis of the digital evidence. A preliminary forensic examination is a brief review taking no more than a couple of hours, whereas a full forensic examination may take anywhere from an entire day to several weeks, depending on the amount of recoverable information. I conducted preliminary forensic examinations on a number of items of evidence seized in this case. Evidence collected from FOB Hammer and delivered to me at Camp Liberty included: two Supply Annex computers, a rewriteable CD, an Apple brand personal laptop, an external hard disk drive, and three Sensitive Compartmented Information Facility (SCIF) computers.

5. I follow several general procedures when handling evidence. I review the custody document and always ensure the description of the evidence matches the evidence attached. I check, for example, that recorded serial numbers, markings for identification, and condition description match the associated evidence. I ensure that the necessary information, such as date and time, are properly and accurately recorded. Lastly, I maintain secure custody of the evidence prior to transferring it to another individual. In addition to following these procedures, when transferring to or receiving evidence from another person, I am also sure to properly sign, date, and note the reason for the transfer.

6. With regard to each item of physical evidence I received in this case, I followed these same procedures. When receiving whole computers, I also checked to ensure they did not contain any suspicious hardware or removable data storage devices such as SD cards and thumb drives. Prior to powering on or accessing the contents of any device, I imaged each item of physical evidence I received in order to preserve the contents of the data on the item. A forensic image of an item of digital media is an exact, bit-for-bit copy of the data on the digital media. I imaged these items of evidence so that the data on the device can be forensically examined without manipulating the data contained on the original evidence. This is standard practice by digital forensic examiners. The software forensic examiners use to image the digital evidence has built in procedures to verify that the item has been successfully duplicated. For example, the program will note the MD5 Hash or Secure Hash Algorithm 1 (SHA1) hash value of an item of digital evidence before imaging (acquisition hash value) and after imaging the item (verification hash value). If the two hash values match, the item has been successfully duplicated bit-for-bit. The hash value is determined by mathematical algorithm and is displayed as a number/letter identifier unique to every item of electronically stored information. It is similar to a digital fingerprint,

although more unique. When the hash value is generated, the entire hard drive will have a hash value, as well as each individual file on the hard drive. If there is any alteration to the hard drive or to any file on the hard drive, the acquisition and verification hash values will not match. The alteration can be as small as adding a single space into a text document or saving a file in a different format (i.e. saving a ".doc" as a ".pdf"). In this case, I used EnCase forensic software to complete this imaging process. EnCase forensic software is widely used by digital forensic examiners. As I stated earlier, I have received training on EnCase forensic software and have used it in my other cases involving digital forensic examinations. I encountered no errors while conducting the imaging of the evidence at issue in this case.

7. Between 30 May 2010 and 1 June 2010, I processed the following items of physical evidence:

a. I processed a Hitachi brand laptop computer, with the serial number 070817DP0C10DSG21DP, which was collected from the Supply Office or Annex, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was marked "UNCLASSIFIED" and was seized because PFC Manning had temporarily worked in the Supply Office in May 2010 and used this computer. I received this evidence from SA Thomas Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed this computer and obtained an EnCase forensic image of the hard drive contained within this computer. The resulting forensic image, with the SHA1 hash value of 309df99f068fba2e81aae03dla93d471cde90bf0, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. I did not examine this image further. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

b. I processed a Seagate brand computer hard drive, with the serial number CN-0MN922-21232-793-002L, which was collected from the Supply Office/Annex, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was connected to the SIPRNET and the hard drive was seized because PFC Manning had temporarily worked in the Supply Office in May 2010 and used this computer. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed this hard drive and obtained an EnCase forensic image of the hard drive. The resulting forensic image, with the SHA1 hash value of cf6d703f0023773eb9e30eeb318660ac0d18f404, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. I did not examine this image further. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

c. I processed a rewriteable compact disc (CD-RW), with the serial number LD623MJ04184038B16, which was collected from the quarters of PFC Manning, Room 4C93, LSA Dragon, FOB Hammer, Iraq. A CD-RW is different from a commercially-produced CD with content already loaded onto it (i.e. from a music store), because a CD-RW allows the user to write content to the CD, along with edit or delete information on the CD. This CD-RW had a

"SECRET" sticker on it and was labeled "12 Jul 07 CZ ENGAGEMENT ZONE 30 GC". This CD-RW was collected with three Arabic language CDs in a multi-disc case. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the multi-disc case and obtained an EnCase forensic image of the aforementioned CD-RW. The resulting forensic image, with the MD5 hash value of 5c993ee621b036482bae1353f844322f, was verified to be an exact, bit-for-bit copy of the CD-RW through a comparison of the acquisition and verification hash values. After imaging this CD-RW, I conducted a preliminary forensic examination of this image. The CD-RW contained two files with identical names. One file contained no data and the other file, "12 Jul 07 CZ ENGAGEMENT ZONE 30 GC," contained a video. The video appeared to have been burned to the disc on 27 April 2010 using Macintosh disc creation software. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

d. I processed an Apple brand laptop computer, with the serial number W8939AZ066E, which was collected from the quarters of PFC Manning, Room 4C93, LSA Dragon, FOB Hammer, Iraq. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Macintosh computer, removed a Fujitsu brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was K94DT9829WPY. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of 3cf107db8b3865a5e3ebfce400bac1da9691fb49, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. Thereafter, I conducted a preliminary forensic examination of this image. I determined that the hard drive had a Macintosh operating system installed and had a user account resembling PFC Manning's name, although I did not note the machine's username in my Agent's Investigation Report (AIR). A review of the device logs contained on the hard drive revealed some form of optical disc (i.e. CD-RW drive) activity occurred, like deleting or burning CD-RWs, on or around 27 April 2010. I also reviewed the "user" files associated with the account resembling PFC Manning's name and located several files containing text that was specifically referenced in the chat logs received by U.S. Army CID during the initial phases of the investigation, though I did not specifically note which text was referenced in the chat logs in my AIR. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

e. I processed a Seagate brand external hard disk drive (HDD), with the serial number 2GEWJKLJ, which was collected from the quarters of PFC Manning, Room 4C93, LSA Dragon, FOB Hammer, Iraq. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the external HDD case and further removed the internal HDD, also Seagate brand (serial number 9VS1S2TZ), because I did not have a power adapter that could safely and reliably power the Seagate brand external HDD. I then obtained an Encase forensic image of the internal Seagate HDD with the SHA1 hash value of 151183463c5b5841a8115627bf51e8d9e74abb48. The resulting forensic

image was verified to be an exact, bit-for-bit copy of the Seagate HDD through a comparison of the acquisition and verification hash values. After imaging the Seagate HDD, I conducted a preliminary forensic examination of this image. I found a file containing the contact information of a member of the WikiLeaks team, Mr. Julian Assange. This contact information appeared to have been produced and released by the WikiLeaks team and did not appear to be of a personal nature. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

f. I processed an Alienware brand laptop computer, with the serial number NKD900TA6D00661, which was collected from the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was connected to the SIPRNET and the hard drive was seized because PFC Manning had worked in the SCIF in November 2009 to May 2010 and used this computer. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Alienware laptop computer, removed the Seagate brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was 3MH036M1. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of c7400fbbed0b4db68a582a585eeaa34ab1a62cd64, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. Thereafter, I conducted a preliminary forensic examination of this image. I determined that PFC Manning had a user account on this laptop computer. I found several items of interest to this investigation, including copies of the Apache video made publicly available by WikiLeaks and called "Collateral Murder." I also found an archive file that contained approximately 11,000 sensitive and classified documents, downloaded in Hyper Text Markup Language (HTML) format, though I did not note the exact number. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

g. I processed a Dell brand laptop computer, with the serial number HLVJQF1, which was collected from the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was connected to the SIPRNET and the hard drive was seized because PFC Manning had worked in the SCIF in November 2009 to May 2010 and used this computer. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Dell laptop computer, removed an unknown brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was 5MH0HWKN. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of c3473c3df1d131e0022f0c56bfc46087e9d5150f, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. Thereafter, I conducted a preliminary forensic examination of this image. I determined that PFC Manning had a user account on this laptop computer. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

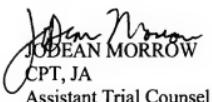
h. I processed a Dell brand laptop computer, with the serial number 93H4QD1, which was collected from the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This NIPRNET laptop had been located near the work area of PFC Manning. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Dell laptop computer, removed an unknown brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was 5MH0TB78. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of e2b49bd3ed0c2f5d798ab44febaac3b15d0070be, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. I did not examine this image further. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

8. As I stated earlier, I used the EnCase forensic software to obtain the images of each item of evidence I processed. In this case, I attached each device (except the CD-RW) to a write-blocker, and then attached the write-blocker to my laptop computer, which had the EnCase forensic software loaded. A write-blocker is a device that allows you to acquire information on an item of digital media without accidentally damaging or altering the contents of the original item of digital media. In short, the write-blocker ensures that none of the original data on the item of evidence is manipulated in any way. I did not use the write-blocker when processing the CR-RW, as that device was not at risk of alteration. Computers do not alter data on CD-RWs without specific instructions to do so. As I neither intended nor actually issued such instructions, there was no need to use a write-blocker with regards to the CD-RW. After securing the write-blocker as appropriate, I then used EnCase to create a forensic image of each item. As I stated earlier, EnCase creates an acquisition hash value that is later compared to the verification hash value once the image has been created. I saved the forensic images of each device I processed onto sterile hard drives. I later transferred these forensic images to the hard drives recorded as Items 1 and 2 on DN 073-10. The forensic image is not altered by being transferred between storage devices. When you open the forensic image in EnCase, EnCase itself verifies that the forensic image is a true copy.

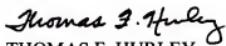
9. Item 1 of DN 073-10, serial number 9VS25G5M, is a Seagate brand hard disk drive containing the individual forensic images of the devices listed above that were initially determined to be "UNCLASSIFIED." Item 2 of DN 073-10, serial number 5VG1826C, is a Seagate brand hard disk drive containing the individual forensic images of the devices listed above that were initially determined to be classified "SECRET." On 5 June 2010, I collected Items 1 and 2 as evidence because I had previously transferred the forensic images of the various devices I processed to these two hard disk drives. I collected this evidence at the CID office on Camp Liberty. I did this to consolidate the evidence I processed for ease of review by subsequent forensic examiners. This process is consistent with best computer forensic practices. In the forensic community, it is common for investigators to consolidate the forensic images of multiple devices on one hard drive and then collect the resulting hard drive as evidence. After I collected Items 1 and 2 as evidence, I transferred custody of this evidence to SA Jeremy Drews.

10. During the above forensic examinations, I recorded my notes, including descriptions of the evidence and their associated hash values on an AIR, dated 5 June 2010, and marked for this court-martial with bates numbers: 00021674 - 00021683. This AIR accompanied the evidence I transferred to SA Drews.

11. Prosecution Exhibit 11 for Identification is the Seagate brand hard disk drive with serial number 9VS25G5M (Item 1 of DN 073-10). Prosecution Exhibit 12 for Identification is the Seagate brand hard disk drive with serial number 5VG1826C (Item 2 of DN 073-10).



JODEAN MORROW
CPT, JA
Assistant Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused

You can currently contact our investigations editor directly in Iceland +354 862
3481 ; 24 hour service; ask for "Julian Assange".

ManningB_00125284

PROSPECTIVE PUBLIC RELEASE DATE: 24 JUNE 2012
PAGE 1 OF 1, APPROXIMATELY 1 PAGES
PAGE 1 OF 1, APPROXIMATELY 1 PAGES

UNCLASSIFI

D

Pvt Manning, Bradley

D Company, 305th Military Intelligence Battalion

Friday, 13 Jun 08

UNCLASSIFI

D

UNCLASSIFI

D

Executive Summary

- Definition of OPSEC
- Types of OPSEC Information
- Common OPSEC Violations
- Protection from Adversaries
- Conclusion

UNCLASSIFI

D

UNCLASSIFI

D

Definition of OPSEC

- Operations Security (OPSEC)
- Protection of Information:
 - Public Assets
 - Military Assets
 - Personnel
 - Families of Personnel
 - National Security

UNCLASSIFI

D

UNCLASSIFIED

D

Types of Information

- Unclassified Information
 - Dates
 - Times
 - Locations
 - Names
- For Official Use Only (FOUO)
 - Mission Critical Information
 - Capabilities
 - Vulnerabilities

UNCLASSIFIED

D

UNCLASSIFI

D

Dates and Times

- Events
 - Large groups
 - . Public
 - . Military Personnel
 - . Department of Defense Civilians
 - . Contractors
 - Officials
 - . High Ranking NCO's
 - . Commanders
 - VIP's
 - . Politicians
 - . Diplomats

UNCLASSIFI

D

UNCLASSIFI

D

Location Information

- Government Facilities
 - Public Buildings
 - Government Agencies
- Military Installations
 - Secure Facilities
 - Weapons and Equipment
 - Training Locations
 - Barracks

UNCLASSIFI

D

UNCLASSIFI

D

Individual Information

- Personal Information
 - Names
 - Dates of Birth
 - Addresses
 - Social Security Numbers
 - Credit Information
 - Family Members

UNCLASSIFI

D

UNCLASSIFI

D

Official Information

- Methods
 - Intelligence Gathering
- Equipment
 - Weapons
 - Vehicles
- Capabilities
- Vulnerabilities
- Mission Critical Information

UNCLASSIFI

D

UNCLASSIFI

D

Adversaries

- . Foreign Governments
 - Rivals
 - Enemies
- . Non-Government Organizations
 - Corporations
 - Political Groups
 - Terrorists
- . Anyone
 - Activists
 - Hackers

UNCLASSIFI

D

UNCLASSIFI

D

Common OPSEC Leaks

- Written Sources
 - Newspapers
 - Magazines
- Television
 - News Programs
 - Documentaries
- Internet
 - Discussion Boards
 - Chat Rooms
 - Social Networking
 - Videos

UNCLASSIFI

D

UNCLASSIFI

D

Conclusion

- Avoid Disclosure of Information
 - Public Conversations
 - Journalists
 - Posting Information
 - . Newsletters
 - . Fliers
 - . Internet
- Use Common Sense
 - Many Enemies
 - Free and Open Society

UNCLASSIFI

D

UNCLASSIFI

D

UNCLASSIFI

D

UNITED STATES OF AMERICA

v.
Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
STIPULATION OF
EXPECTED TESTIMONY

)
SA Antonio Edwards

)
DATED: 3 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent (SA) Antonio Edwards were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows.

1. Since March of 2012, I have been employed as a Special Agent ("SA") of Homeland Security Investigations ("HSI"), Department of Homeland Security ("DHS") in the Atlanta Field Office, empowered by law to investigate and to make arrests for offenses involving the unlawful export of goods and technology to destinations outside the United States. Prior to working for HSI, from March 2008 to March 2012, I was employed as an SA with the United States Army Criminal Investigation Command ("USACIDC"), Computer Crime Investigative Unit ("CCIU") at Fort Belvoir, Virginia. In this capacity, I was responsible for the investigation of violations pertaining to computer intrusions and to other types of malicious computer activity directed against the U.S. Army (18 U.S.C. § 1030). As a USACIDC SA, I was also authorized to investigate crimes involving all violations of the Uniform Code of Military Justice and other applicable federal and state laws where there is a U.S. Army or Department of Defense (DoD) interest. I have participated in and conducted investigations of violations of United States laws and regulations pertaining to computer intrusions and I have participated in the execution of search warrants on individuals and companies.
2. Before working for USACIDC, from November 2007 to November 2008, I was employed as an SA with the Bureau of Industry and Security (BIS), Office of Export Enforcement. And, from May 2003 to October 2006, I was a Deputy Prosecutor for Morgan County, Indiana. From August 2000 to August 2005, I served in the Monroe County, Indiana Reserve Deputy Sheriff's Department as a Deputy Sheriff, where I received training in evidence collection. Further, I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program, where I also received training in evidence collection. In addition to being employed as a Special Agent, I currently serve in the Inactive Ready Reserves (IRR) as a Judge Advocate in the United States Army National Guard, District of Columbia.
3. In 2003, I received a Juris Doctorate from Indiana University and was subsequently admitted to the Indiana bar. I have a Bachelor of Arts in Psychology from the University of North Florida, and a Doctorate of Jurisprudence from Indiana University – Bloomington School of Law. I am currently licensed to practice law in Indiana.
4. My experience as a State Law Enforcement Officer, a State Prosecutor, and a Special Agent has included the investigation of cases involving violent and non-violent crimes as well as the use of computers. I have also received training and gained experience in: interviewing and interrogation techniques, arrest procedure, crime scene examination, evidence collection, search warrant applications, the execution of searches and seizures, and other criminal laws and procedures. Further, I have completed the Department of Defense Cyber Investigations Training Academy courses: "Introduction to Computer Hardware", "Computer Incident Responders Course", and "Windows Forensic Examinations – EnCase".

Together, this afforded me certification as a Department of Defense "Certified Digital Media Collector" and "Certified Digital Forensic Examiner".

5. I follow several general procedures when handling evidence. I review the custody document and always ensure the description of the evidence matches the evidence attached. I check, for example, that recorded serial numbers, markings for identification, and condition description match the associated evidence. I ensure that the proper information, such as date and time, are properly and accurately recorded. Lastly, I maintain secure custody of the evidence prior to transferring it to another individual.
6. In this particular investigation, I assisted with witness interviews and the handling of evidence. In so doing, I worked with SA Charles Clapper and Mr. Garon Young. On 12 June 2010, I received several pieces of electronic evidence related to this investigation from the hands of Mr. Adrian Lamo and with his consent. On 12 June 2010, Mr. Adrian Lamo also gave signed consent to law enforcement personnel on two separate CID Forms 87-R-E to search his electronic devices for "[a]ll information in any form, pertaining to communications which may be in the form: of emails, instant messaging chats, documents, data, computer code, log files, drawings, photographs, or any other data; in encrypted, plain text, or any other format; relating to PFC Bradley E. MANNING and/or the disclosure of classified information or information which is the property of the U.S. Government." The first piece of evidence collected and further handled was a Lenovo Laptop computer with a Fujitsu computer hard drive (serial number: K4047812MF4D) recorded as Item 1 on a DA Form 4137 marked as document number (DN) 76-10, and known as "Lamo Ubuntu Hard Drive". It was collected from Mr. Adrian Lamo in Sacramento, California on 12 June 2010. The second piece of evidence collected and further handled was an HP Mini Brand computer (computer serial number: CNU90513VT) with a Seagate computer hard drive (hard drive serial number: 5RE2C1QK) recorded as Item 1 on a DA Form 4137 marked as document number (DN) 77-10, and known as "Lamo HP Hard Drive". It was collected from Mr. Adrian Lamo in Carmichael, California on 12 June 2010.
7. Using the DA Form 4137, I properly released these pieces of evidence to SA Clapper. On 14 June 2010, I properly regained possession from SA Clapper before properly releasing them to the Evidence Custodian, Mr. Garon Young, on 15 June 2010, which is documented on a DA Form 4137. While in possession of these items, I maintained control over them, stored them properly, and allowed no one else access to them. I did not alter the evidence in any way. I have no reason to believe this evidence was damaged or contaminated in any way. After releasing the evidence to Mr. Young, I had no further interaction with the evidence.

8. Prosecution Exhibit 13 for Identification is the Lamo Ubuntu Hard Drive (Item 1 of DN 76-10). Prosecution Exhibit 14 for Identification is the Lamo HP Hard Drive (Item 1 of DN 77-10).



ASHDEN FEIN
MAJ, JA
Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

STIPULATION OF
EXPECTED TESTIMONY

SA Charles Clapper

DATED: 3 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent (SA) Charles Clapper were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows.

1. I am a Special Agent (SA) for the U.S. Army Criminal Investigation Division (CID). Specifically, I work for the CID, Computer Crimes Investigation Unit (CCIU). My current job title is Special Agent in Charge (SAC) of the Arizona Branch Office located at Fort Huachuca, Arizona. As the SAC, I run a two-man office that handles exclusively computer crimes. My job also entails serving as CID's liaison officer for NETCOM. Additionally, I am the liaison officer to the Regional Computer Emergency Response Team (RCERT-CONUS) and to the Theater Network Operations and Security Center (TNOSC). I have served in Arizona as an SA for five years and I have been the SAC for three of the five years.
2. From 1986-1999, I was an enlisted Military Police officer (MP). I served as an Evidence Custodian for the Investigation Section at Fort Lewis, Washington from 1993-1994. After becoming a CID agent in 1999, from 1999-2002, I served as the Computer Crimes Coordinator for the 5th MP Battalion in Kaiserslaughtern, Germany. I was also the Evidence Custodian for the Kaiserslaughtern CID Office from 2001-2002. I served as the Detachment Sergeant and as an Evidence Custodian from 2004-2006 at CCIU on Fort Belvoir, Virginia. In 2007, I was an INSCOM contractor performing forensics for the Army's Computer Emergency Response Team (Army CERT) in the Forensics and Malware Analysis department. I became a civilian Special Agent in Arizona in 2008, and currently serve in this capacity.
3. I received a Bachelor of Science degree in Liberal Arts from Regents College located in New York. I have had extensive training in evidence collection and handling. This includes having attended the 17-week Apprentice Special Agents Course. I have also attended the Advanced Crime Scene Investigation class at Fort Leonard Wood and the SALT Special Agent Course at the Army Crime Lab located at Fort Gillem, Georgia. In terms of computer and forensic training, I have taken numerous courses at the Defense Cyber Investigative Training Academy in Linthicum, Maryland. I took these courses between the years 2000 and 2008. They covered a full range of computer forensics and digital media collection issues. Between 2003 and 2006, I attended two courses at Guidance Software in Reston, Virginia. This company manufactures the forensic imaging software EnCase. In 2012, I attended the Federal Law Enforcement Training Center Computer Network Intrusion Training program in Glynnco, Georgia. These courses all discussed the collection and handling of digital evidence.
4. I have a Department of Defense Cyber Crime Investigation Certificate from the Department of Defense Cyber Crime Center, which is the highest certification that one can receive in the field.

The certification must be renewed every two years. I received my first certification in 2006 and last renewed it in October of 2012. In addition to my training and certifications, I have worked more than 100 cases in my current duty position and somewhere between 100-200 cases in my previous capacities.

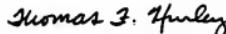
5. I follow several general procedures when handling evidence. I review the custody document and always ensure the description of the evidence matches the evidence attached. I check, for example, that recorded serial numbers, markings for identification, and condition description match the associated evidence. I ensure that the appropriate information, such as date and time, are properly and accurately recorded. Lastly, I maintain secure custody of the evidence prior to transferring it to another individual.

6. In this particular investigation, I worked with SA Antonio Edwards and assisted with witness interviews and the handling of evidence. On 12 June 2010, I received evidence related to this investigation from SA Edwards. I also received two Consent to Search forms (CID Forms 87-R-E), signed by Mr. Adrian Lamo on 12 June 2010, which gave signed consent to law enforcement personnel to search his electronic devices for “[a]ll information in any form, pertaining to communications which may be in the form: of emails, instant messaging chats, documents, data, computer code, log files, drawings, photographs, or any other data; in encrypted, plain text, or any other format; relating to PFC Bradley E. MANNING and/or the disclosure of classified information or information which is the property of the U.S. Government.” The first piece of evidence collected and further handled was a Lenovo Laptop computer with a Fujitsu computer hard drive (serial number: K404T812MF4D) recorded as Item 1 on a DA Form 4137, marked as document number (DN) 76-10, and known as “Lamo Ubuntu Hard Drive”. It was collected from Mr. Adrian Lamo in Sacramento, California on 12 June 2010. The second piece of evidence collected and further handled was an HP Mini Brand computer (computer serial number: CNU90513VT) with a Seagate computer hard drive (serial number: 5RE2C1QK) recorded as Item 1 on a DA Form 4137, marked as document number (DN) 77-10, and known as “Lamo HP Hard Drive”. It was collected from Mr. Adrian Lamo in Carmichael, California on 12 June 2010.

7. I imaged both pieces of evidence using standard forensic imaging software, which does not alter the original evidence in any way. A forensic image is a bit-for-bit or exact copy of the original information on the hard drive. Using the DA Form 4137, I properly released the original evidence back to SA Edwards on 14 June 2010. While in possession of these items, I maintained control over them. I returned the items in the same condition that I received them and have no reason to believe that the evidence was damaged or contaminated in any way. After releasing the evidence to SA Edwards, I had no further interaction with the evidence.



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel



Thomas F. Hurley
THOMAS F. HURLEY
MAJ, JA
Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)
)
)

**STIPULATION OF
EXPECTED TESTIMONY**

Mr. Garon Young

DATED: 3 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Garon Young were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I am currently the Criminal Intelligence Program Manager for the U.S. Army Computer Crime Investigative Unit (CCIU) of the Criminal Investigative Division (CID). I have been with CCIU for 10 years. This position primarily entails reviewing cases for intelligence data and entering them into our database. Additionally, I review reports, serve as the security manager, and act as alternate evidence custodian. I have held this position for 10 years.
2. I have an Associate's degree from Central Texas College and began my law enforcement career in 1980 as a Military Policeman. In 1987 I became a Military Police Investigator. From 1989 to 1992, I was the Chief of Investigations in Wuerzburg, Germany. During this time (1989 - 1991), I was also the evidence custodian. I joined CID in 1993 and from 1994 to 1995 was the alternate evidence custodian while stationed in Korea. From 1995 to 1998, I was the detachment sergeant at Fort Leonard Wood. In this capacity, I was the senior enlisted advisor and primary evidence custodian. From 1998 until I retired in 2000, I worked at CID Headquarters on Fort Belvoir. After 3 years of working for the Florida Department of Revenue, in 2003, I returned to criminal investigations by joining CCIU. I have worked in my current position since then - serving from 2003 to 2006 as the alternate and occasionally primary evidence custodian at various times. Throughout my years in law enforcement, I have worked more than 800 cases.
3. In 1996, I took the Medical Legal Death Investigations Training by the Armed Forces Institute of Pathology held at Fort Lewis. In 2005, I attended the Evidence Management Course at the United States Army Crime Lab in Fort Gillem, GA. And in 2007, I returned to Fort Gillem for the Army Crime Lab's Special Agent Laboratory Training. These courses do cover physical and digital evidence collection and handling.
4. I follow several general procedures when handling evidence as evidence custodian. The first time I receive a piece of evidence I check the accompanying DA Form 4137 evidence custody document to make sure the evidence matches the description and that the marked-for-identification number on the evidence matches what is recorded on the form. I also check to make sure the form has been appropriately filled out. When I sign the evidence into the evidence room, I sign in the "received" column. I then log it in the evidence book and the database before placing it in the evidence room. When someone asks to receive a stored piece of evidence, I pull the voucher number and locate the evidence in its appropriate location. I check to make sure the evidence I am handing over matches the description on the form and then I release it to the

Special Agent or Forensic Examiner who has requested it. I sign that I have released it and the individual receiving it signs that (s)he has received it. Each time I relinquish or assume custody of evidence, I check the description to make sure the evidence being transferred matches the forms used to transfer it.

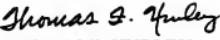
5. In my capacity as evidence custodian I have worked with SA Kirk Ellis, SA Antonio Edwards, and Ms. Tamara Mairena. When Ms. Mairena came on board as the primary evidence custodian, I trained her. She works as the primary and I as the alternate evidence custodian. It is normal for her to sign evidence out of the evidence room and for me to sign it back in (or vice versa).

6. I am involved in the present case because of my role in assisting the investigation team with the secure storage of the evidence they collect. I have received evidence from both SA Edwards and SA Ellis.

7. On 15 June 2010, I received evidence related to this investigation from SA Edwards. I took custody of a Lenovo Laptop computer with a Fujitsu computer hard drive (serial number: K404T812MF4D), collected from Mr. Adrian Lamo while in Sacramento, CA on 12 June 2010, recorded as Item 1 on a DA Form 4137 marked as document number (DN) 76-10, and known as: "Lamo Ubuntu Harddrive". I also took custody of an HP Mini Brand computer (computer serial number: CNU90513VT) with a Seagate computer hard drive (hard drive serial number: 5RE2C1QK), collected from Mr. Adrian Lamo in Carmichael, CA on 12 June 2010, recorded as Item 1 on a DA Form 4137 marked as DN 77-10, and known as "Lamo HP Harddrive". Upon taking possession of this evidence I logged it in to the evidence room using the proper procedures I just described. I never logged it back out.

8. On 15 June 2010, I also received evidence related to this investigation from SA Ellis. I took custody of a DVD (Marked "0028-10-cid221-10117 Dept of State Server Logs, 199.56.188.73"), seized from the Department of State on 15 June 2010, recorded as item 1 on a DA Form 4137 marked as DN 78-10, and known as "DoS Server Logs". Upon taking possession of this evidence, I logged it into the evidence room using the proper procedures I described earlier. I never logged it back out.


ASHDEN FEIN
MAJ, JA
Trial Counsel


THOMAS F. HURLEY
MAJ, JA
Defense Counsel


BRADLEY E. MANNING
PFC, USA
Accused

UNITED STATES OF AMERICA)
v.)
Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

STIPULATION OF
EXPECTED TESTIMONY

Ms. Tamara Mairena

DATED: 3 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Ms. Tamara Mairena were present to testify during the merits and pre-sentencing phases of this court martial, he would testify substantially as follows:

1. I am the primary evidence custodian at the Computer Crimes Investigative Unit (CCIU) of the U.S. Army Criminal Investigation Command (CID) in Quantico, Virginia. I have held this position since 2006. In this position, I track and catalog evidence maintained by our CCIU office.
2. I have been a Certified Evidence Custodian since January of 2006. I received this certification from the U.S. Army Criminal Investigation Laboratory. Since January 2010, I have also been a Department of Defense (DOD) Cyber Investigations Training Academy certified digital media collector.
3. I follow several general procedures when handling evidence as evidence custodian. The first time I receive a piece of evidence, I check the accompanying DA Form 4137 evidence custody document to make sure the evidence matches the description and that the marked-for-identification number on the evidence matches what is recorded on the form. I also check to make sure the form has been appropriately filled out. When I sign the evidence into the evidence room, I sign in the "received" column. I then log it in the evidence book and the database before placing it in the evidence room. When someone asks to receive a stored piece of evidence, I pull the voucher number and locate the evidence in its appropriate location. I check to make sure the evidence I am handing over matches the description on the form and then I release it to the Special Agent or Forensic Examiner who has requested it. I sign that I have released it and the individual receiving it signs that (s)he has received it. Each time I relinquish or assume custody of evidence, I check the description to make sure the evidence being transferred matches the forms used to transfer it.
4. I first became involved in the present case because of my role in assisting the investigation team with the secure storage of evidence they collect. I signed several pieces of evidence from the investigating agents and forensic examiners into the evidence room and would release evidence back to them when they needed it for their investigation or examinations. In my role as evidence custodian, I have worked with and received evidence from Special Agent Kirk Ellis, Special Agent Antonio Edwards, Special Agent David Shaver, Special Agent Calder Robertson, Special Agent John Wilbur, and Special Agent Mark Mander. I also know Mr. Garon Young. He used to be the primary evidence custodian and trained me when I began working for Army

CCIU. Mr. Young currently serves as the alternate evidence custodian. As such, it is normal for him to sign something out of the evidence room and for me to sign it back in (or vice versa).

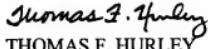
5. On 18 June 2010, I signed a Lenovo laptop computer with Fujitsu computer hard drive (serial number: K404T812MF4D), collected from Mr. Adrian Lamo in Sacramento, California on 12 June 2010, recorded as Item 1 on a DA Form 4137 marked as document number (DN) 76-10, and known as "Lamo Ubuntu Harddrive" out of the evidence room to SA Dave Shaver for forensic examination. I also signed out an HP Mini Brand computer (computer serial number: CNU90513VT) with Seagate hard drive (serial number: 5RE2C1QK), collected from Mr. Adrian Lamo in Carmichael, California on 12 June 2010, recorded as Item 1 on a DA Form 4137, marked as DN 77-10, and known as "Lamo HP Harddrive" to SA Shaver for the same reason. He returned these items later that same day. I received and released this evidence according to the proper procedures I just described. I did not alter this evidence in any way.

6. On 18 October 2010, I received evidence related to this investigation from SA Wilbur, recorded as Item 1 on a DA Form 4137 marked as DN 151-10. I took custody of a CD (marked "Wikileaks DoS Firewall Logs 13 Oct 10") collected from the Department of State on 15 October 2010, and known as "DoS Firewall Logs". Upon receiving this evidence, I properly logged it into the evidence room using the same procedures described earlier. On 1 November 2010, I properly released it to SA Shaver for examination. He returned it later that same day. I received and released this evidence according to the proper procedures I described earlier. I did not alter this evidence in any way.

7. On 3 November 2010, I received nineteen pieces of evidence from SA Mander, collected from the home of Ms. Debra Van Alystne in Potomac, Maryland on 2 November 2010, recorded as Items 1-19 on a DA Form 4137 marked as DN 162-10. Item 2 on this DA Form 4137 was an SD memory card (serial number: BE0915514353G), known as "SD Card". On 10 December 2010, I properly released the "SD Card" to SA Shaver for examination. He returned it later that same day. I properly received the evidence back in to the evidence room according to the proper procedures I described earlier. I did not alter this evidence in any way.



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused

Prosecution Exhibit 30

50 pages

classified

"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order

dated 20 August 2013
stored in the classified
supplement to the original
Record of Trial

00527869

https://twitter.com/wikileaks/status/13570878440

2 results (0.09 seconds)

Ad referred to https://twitter.com/wikileaks/status/13570878440 (.)
The Silver of WikiLeaks - What's the real secret behind
www.facebook.com/WikiLeaksSecrets
WikiLeaks and Julian Assange?

Twitter/wikileaks. Who would like a list of us...
https://twitter.com/wikileaks/status/13570878440 =
https://twitter.com/wikileaks/status/13570878440 -
March 9, 2010 - why is WikiLeaks collecting military email addresses? (Assumed) - viewed
like a list of us - http://Twitter.com/wikileaks/status/13570878440 -

Advanced search Search Help Send feedback

Google Home Advertising Programs Business Solutions Privacy & Terms About Google

PROSECUTION EXHIBIT 31 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE OF PAGES

92

0
0
5
2
7
8
7
0

Twitter / WikiLeaks

webcache.googleusercontent.com/search?q=cache:JQ+OjzjRWWPlF0TBzLhttps://twitter.com/wikileaks/status/1570878401+https://twitter.com/wikileaks/status/1570878401&cd=1&gl=en&tz=canberra

Search

WikiLeaks (@wikileaks)

We would like a list of as many .mil email addresses as possible. Please contact editor@wikileaks.org or submit

Reply 13 Retweet 5 Favorites 48 More

27 RETWEETS 5 FAVORITES

2.37 PM · Mar 10

Don't miss any updates from WikiLeaks

Join Twitter today and follow what interests you!

Full name Email Password

Test follower address in 40404 in the United States

Sign up

© 2013 Twitter About Help

WikiLeaks WikiLeaks WikiLeaks WikiLeaks

<http://twitter.com/#!/wikileaks/status/13570878440>



PAGE 31 OF 33

31
ADMISSIONS

22

File Edit View Favorites Tools Help

Army Knowledge Online GFEIS Login Outlook Web App Accounts Find People Purchasing Research School Personal

https://twitter.com/wikileaks/status/1357057640

Track y... M Index - "http:// Twitter... WML Making... Twitter... Sign in

Search

Follow

WikiLeaks @wikileaks

We would like a list of as many .mil email addresses as possible. Please contact editor@wikileaks.org or submit

Reply 13 Retweet Favorite More

37 RETWEETS 9 FAVORITES

2:37 PM - 7 May 10

Don't miss any updates from WikiLeaks
Join Twitter today and follow what interests you!

Full name Email Password

Text follow wikileaks to 40404 in the United States

Sign up

© 2013 Twitter About Help

PROSECUTION EX-IBIT 31b for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE _____ OF _____ PAGES

02

00527871

PROSECUTION EXHIBIT 32 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE ____ OF ____ PAGES

Google https://twitter.com/leakstatus/7530875613

About 203 results (0.13 seconds)

Ad related to https://twitter.com/leakstatus/7530875613 ⓘ

The Site of WikiLeaks - What's the most secret leaked
www.facebook.com/RecycleSecrets
Wikileaks and Julian Assange

Twitter / WikiLeaks_Hans_sizecreasedvideo_at_15s
http://twitter.com/wikileaks/status/7530875613
Apr 1 2010 - Don't worry, we've sizecreased this video from Twitter today and taken what
you need... You'll have to follow us @wikileaks in the United States

Twitter / Zedninja: http://twitter.com/zedninja
twitter.com/zedninja/status/11799335496
Apr 1 2010 - As you all might have heard, WikiLeaks created a surveillance video -
processing video file: http://twitter.com/zedninja/status/7530875613

References :: News from WikiLeaks world :: Topic created by
www.ethicalhacker.net/component?option=com_smf&Itemid=54 / Apr, 5336 0/
Apr 1 2010 - As you all might have heard, WikiLeaks created a surveillance video -
processing video file: http://twitter.com/zedninja/status/7530875613

Salon.com Mobile | NY Times: WikiLeaks Stole 100,000 in a heartbeat
letters mobile salon.com / 04d7676e82ebfb4c1bc4acfc67c29c59d.html
Apr 1 2010 - http://twitter.com/zedninja/status/7530875613 Have encrypted video of
WikiLeaks video or don't know who to thank? Go to next page

WikiLeaks video "crisis" - Gmail
http://www.youtube.com/watch?v=qCwzvxcng encrypted general0138656
Apr 1 2010 - Instead of trying to figure out how to get the video and other
info, http://twitter.com/zedninja/status/7530875613 The video was...

Gmail attachments download attachments_email02
blog.gmane.org/mime_comp_encrypted/general010401 =
Apr 1 2010 - Indeed, WikiLeaks requested "supercomputer keys" via letter and other means to
decryt a video, see http://twitter.com/zedninja/status/7530875613

From: attachment at email.com What: Apr 1 2010 12:09:26.2010 EDT
www.matzschke.com/cryptopedia/cryptography/2010/04/01 =
Indeed, WikiLeaks requested "supercomputer keys" via letter and other means to
decryt a video, see http://twitter.com/zedninja/status/7530875613

decryption@matzschke.com 11452146 in cryptowebmaster@212.net.mail ...
decosmit@mit.edu@kamikaze@cryptor145214 =
Apr 1 2010 - In the WikiLeaks video "crisis" ... letter and other means to "decryt" a
video, see http://twitter.com/zedninja/status/7530875613 ... The letter ...

WikiLeaks Protecting Anonymous Whistleblowers Archives
https://ptl.secure.hostingprod.com/~7wkaiaj/pvtcrypto-anonymous-w...
Apr 1 2010 - WikiLeaks Protecting Anonymous Whistleblowers Archives on the internet;
User name: ... http://twitter.com/zedninja/status/7530875613 ...

http://www.google.com/search?hl=en
tiny.cc/040cmw-search.cgi?bq_id=145&qj_lml=20
Sep 3 2011 - WikiLeaks Twitter feed apparently violates US diplomatic code about
Assassins. By ... http://twitter.com/zedninja/status/7530875613 ...

00572872

Twitter / WikiLeaks News

webcache.googleusercontent.com/search?q=cache:YK2LqfAChmpmHtHdLc4vJmzgZDQw13+vegez/HuUyem7wmozvntaz/2-0101140145&hl=en&tbo=d

Search Move to a different Stream

Test site version

 WikiLeaks

Have encrypted videos of US bomb strikes on civilians <http://bit.ly/wlafghan2> we need super computer time <http://ljsf.org/>

[Reply](#) [123 Retweets](#) [Favorites](#) [More](#)

148 RETWEETS 36 FAVORITES 

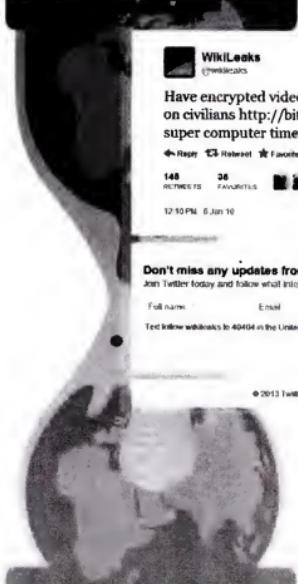
12:50 PM - 6 Jan 10

Don't miss any updates from WikiLeaks
Join Twitter today and follow what interests you!

Full name Email Password

Find WikiLeaks in 40404 in the United States

© 2013 Twitter About Help



WikiLeaks WikiLeaks WikiLeaks WikiLeaks

<http://twitter.com/#!/wikileaks/status/7530875613>



7/22

File Edit View Favorites Tools Help

Army Knowledge Online GFEBS Login Outlook Web App Accounts Find People Purchasing Research School Personal

WikiLeaks @wikileaks

Follow

Have encrypted videos of US bomb strikes on civilians <http://bit.ly/wlafghan2> we need super computer time <http://ljsf.org/>

Reply Retweet Favorites More

147 RETWEETS 37 FAVORITES

12:10 PM - 6 Jan 10

Don't miss any updates from WikiLeaks

Join Twitter today and follow what interests you!

Full name Email Password

Text follow [wikileaks](#) to 48404 in the United States

Sign up

© 2013 Twitter About Help

PROSECUTION EXHIBIT 32 b for identification
PAGE OFFERED. GE ADMITTED: _____
PAGE OF PAGES

02

UNITED STATES OF AMERICA)
v.)
Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

STIPULATION OF
EXPECTED TESTIMONY

ELISA IVORY

DATED: 10 May 2013

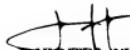
It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mrs. Elisa Ivory were present to testify during the merits and pre-sentencing phases of this court-martial, she would testify substantially as follows.

1. I, Elisa Ivory, previously of the surname Rubin, am the Officer-in-Charge (OIC) of the S-2 section at the 305th Military Intelligence Battalion, Fort Huachuca, Arizona. I have held this position since 2009. As the OIC, I am responsible for security oversight, including those security measures necessary for the in- and out-processing of Advanced Individual Training (AIT) students at the United States Army Intelligence Center and School.
2. Before becoming the OIC of the S-2 section, I was a security specialist in the S-2 section for nearly 15 years. I was the lead for the enlisted section of AIT students and was responsible for processing clearance paperwork, tracking the status of security clearances, and providing the security brief to incoming and outgoing AIT students.
3. All AIT students were required to have a SECRET security clearance to attend AIT. I was responsible for confirming that the AIT students possess the necessary security clearance through the Joint Personnel Adjudication System (JPAS). If any student did not possess a SECRET security clearance, I would process the security clearance, which would include having the student complete a Standard Form (SF) 86. Some Military Occupational Specialties (MOS) required that the student possess a TOP SECRET security clearance in order to graduate AIT, and I would assist those students with processing their TOP SECRET security clearances. PFC Bradley Manning is a 35F (previously 96B) (All-Source Intelligence Analyst), an MOS that required PFC Bradley Manning to possess a TOP SECRET security clearance in order to graduate from AIT.
4. PFC Bradley Manning attended AIT from 4 April 2008 until 14 August 2008, during which time I was a security specialist in the G-2 section. At 0800 on Monday, 7 April 2008, I gave all students, including PFC Manning, a security brief which lasted approximately forty-five minutes. I briefed the class, including PFC Manning, on Operational Security (OPSEC) and Information Systems Security (INFOSEC). Specifically, I briefed that OPSEC is the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conducting of military operations and other activities. Specifically, I briefed that INFOSEC is the system of policies, procedures, and requirements established under the authority of Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. I briefed the class, including PFC Manning, about the dangers to national

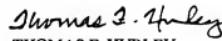
security of allowing U.S. Army and government classified information on the Internet. I explained to the class, including PFC Manning, that putting information on the Internet not only exposes information relating to our national security, but also puts each Soldier at-risk of blackmail by our adversaries given his position of trust to safeguard classified information. During my brief, I discussed previous cases of treason, to include John Walker Lindh and Aldrich Hazen Ames, to teach PFC Manning and the rest of the class the consequences of violating this position of trust and betraying his country.

5. At the conclusion of my security brief, I explained to the class and PFC Manning the purpose and contents of the Standard Form (SF) 312 - Nondisclosure Agreement (NDA). I then asked the class and PFC Manning if they wanted to voluntarily sign the NDA. PFC Manning volunteered to sign the NDA. I then instructed PFC Manning and those others who signed the NDA to stand up, raise their right hand, and state that they accepted the responsibilities contained within the NDA and voluntarily agreed to be bound to the terms within the NDA. Afterwards, PFC Manning completed and voluntarily signed the NDA, for which I co-signed as a witness to PFC Manning's signature.

6. The NDA with BATES # 00022912-00022913 is the NDA which PFC Manning executed on 7 April 2008. The same document is the NDA which I then witnessed PFC Manning sign. I recognize my signature on that specific NDA and I, along with each student for which I co-signed as a witness, followed the above described procedures each time the student executed a NDA.



T. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel



Thomas F. Hurley
THOMAS F. HURLEY
MAJ, JA
Military Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused

UNITED STATES OF AMERICA

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

**STIPULATION OF
EXPECTED TESTIMONY**

SSG Alejandro Marin

DATED: 30 May 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if SSG Alejandro Marin were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows.

1. I, SSG Alejandro Marin, am currently deployed to Afghanistan as a Counterintelligence Analyst in the G-2 (Intelligence) section for the 333d Military Police Brigade. My Military Occupation Specialty (MOS) is 35L, Counterintelligence Agent. My responsibilities in this position include gathering tactical intelligence in our Area of Operation.
 2. From 2002-2006, I was enlisted in the United States Marine Corps with an MOS of Infantry. In July 2007, I enlisted in the United States Army Reserve with an MOS of 11B, Infantry. In early 2008, I reclassified with an MOS of 35F, All-Source Intelligence Analyst. From April 2008 until August 2008, I attended the Intelligence Analyst Course at Advanced Individual Training (AIT) in Fort Huachuca, Arizona. I was assigned to the 305th Military Intelligence Battalion.
 3. PFC Bradley Manning and I attended AIT together. PFC Manning and I were in all of the same classes together at AIT and received the same instruction. The class consisted of approximately 20-25 students, two of whom were PFC Manning and me. I interacted with PFC Manning on a daily basis. Troy Moul was our AIT instructor.
 4. At AIT, I was trained on pattern analysis, which is the study of the enemy's Tactics, Techniques, and Procedures (TTPs) to determine any patterns in enemy activity. I was also trained on how to collect intelligence products and how to map enemy activity as part of pattern analysis. I was also trained extensively on the use of Significant Activities (SIGACTs), which are stored in the Combined Information Data Network Exchange (CIDNE) database on the Secure Internet Protocol Router Network (SIPRNET), a classified network. I was also trained that SIGACTs consist of troop location, Improvised Explosive Device (IED) attacks, and assassinations. Additionally, I was trained on how to research, review, and pull SIGACTs and plot them on a map for pattern analysis.
 5. At AIT, I was trained on the targeting process. I was also trained on how to collect information on High Value Targets (HVTs), to include which databases to use and what type of information is helpful to the targeting process. I was also trained that the intelligence we provided on these HVTs may be employed to carry out military operations to capture these persons. During this instruction, I was also trained on how to use Intelink, a search engine on the SIPRNET similar to Google.

6. At AIT, I was trained on Information Security (INFOSEC). I was also trained on the meaning of classification, to include the different levels of classification. Specifically, I was trained that the unauthorized disclosure of information classified at the SECRET level reasonably could be expected to cause serious damage to the national security and that the unauthorized disclosure of information classified at the CONFIDENTIAL level reasonably could be expected to cause damage to the national security. I was also trained on the meaning of information marked For Official Use Only (FOUO). I was also trained to properly mark not only classified documents at the top and bottom of each document, but also classified media devices with the approved label. I was further trained that we had a personal responsibility to safeguard classified information. I was also trained that access to classified information is limited to those persons with the proper security clearance, signed Non-Disclosure Agreement, and a need-to-know. I was also trained how to store, transmit, and otherwise handle classified information consistent with Army Regulation 380-5.

7. At AIT, I was trained on Operational Security (OPSEC). I was trained not to publicly disclose anything that could be useful to our adversaries, both foreign and domestic. I was also trained on the dangers of putting information on the Internet, to include social media websites. I was also trained on how the enemies of the United States, including Al Qaeda, use the Internet by searching websites for many purposes, such as to collect intelligence on the United States and for use as propaganda and as a recruiting tool. I was trained that OPSEC applies to unclassified information, such as information relating to training schedules and unit morale. At AIT, I was aware that PFC Manning had to give a five minute brief on OPSEC.

8. With regards to BATES numbers 00007351-00007426, 00007450-00007586, 00007629-00007789, 00007983-00008087, 00008152-00008288, 00008331-00008522, 00008853-00009046, 00009802-00010037, and 00010722-00010843, I have reviewed all of these slides. The formatting of the slides is very recognizable to me. As I reviewed the slides, my memory makes me believe that these were the slides that were given to us at AIT. The slides were multiple classes in one presentation. To the best of my knowledge, these slides appear to be the ones used for our classes because of the formatting and content contained in the slideshow. I remember being trained on the content of these slides at AIT, such as memorizing the "CARVERSHP" mnemonic device at BATES number 00010767. However, I cannot say for certain that these are the actual slides or the actual information from the slides given to us due to the length of time that has gone by. It has been five years since I have seen the slides. I also cannot say for certain that these are the slides because not all of the slides were used in all the classes due to time constraints or a class being shortened. At a minimum, these slides are very similar to the slides I received during AIT.

9. At AIT, PFC Manning participated in a Field Training Exercise (FTX), during which PFC Manning created various intelligence products, such as targeting packets on HVTs. I was a team leader during this FTX and had the opportunity to review PFC Manning's work product. PFC Manning's strengths included computer-related tasks, such as pulling data from databases containing intelligence products.

10. I was an All-Source Intelligence Analyst for approximately four years. In 2012, I reclassified with an MOS of 35L, Counterintelligence Agent.


J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel


THOMAS F. HURLEY
Military Defense Counsel


BRADLEY E. MANNING
PFC, USA
Accused



PROSECUTION EXHIBIT 602 for identification
PAGE OFFERED: ____ PAGE ADMITTED: ____
PAGE ____ OF ____ PAGES

ManningB_00199454

Re: Hello Again

Subject: Re: Hello Again
From: Bradley Manning <bradley.e.manning@gmail.com>
Date: Thu, 20 May 2010 01:51:20 +0300
To: Eric Schmiedl <unlocked@MIT.EDU>

You're absolutely right, and I totally agree with you. Though overall, I'm glad it was released, and glad it made an impact. Assange learned a lot from that, and I criticized him.

Though, none of the actual written text in the video is inaccurate. Assange has more material on the topic, which due to source protection paranoia was not released. Some other material is wedged inside of the entire database of events for the Iraq War from 01 JAN 2004 to 31 DEC 2009. Approximately 500,000 incident reports.

He also has 260,000 State Department cables. He's got dirt on every diplomat and head-of-state on the planet from the mid-90s to MAY 1, 2010. I

On 5/20/10 1:35 AM, Eric Schmiedl wrote:

Huh. My objection to "Collateral Murder" is that murder is such a strong word that it overshadows the meaning of a "squishy" word like collateral... so that my reading of the phrase is something like "collateral damage is accidental killing of civilians. This is outright MURDER of civilians." That's a pretty strong accusation to make with no clear evidence that it was intentional (the definition of murder), so in my mind the "collateral murder" tagline reduces the overall credibility.

Basically: right at the beginning, you're making unsupported allegations... how am I supposed to believe the rest?

In comparison, releasing the video without embellishment, and a mere listing of known facts (no firefights in the area, Reuters reporter among the group, etc) lets people put their own interpretation on it. Often, what people imagine is far more shocking than the truth, as horror film directors know all too well... and when you add political blogs to the mix, who knows?

On 5/19/10 6:22 PM, Bradley Manning wrote:
Good question.

There's a few answers I have to various other questions as well:

1. I approved the edits without actually viewing the video. (Had a written description.)
2. I "saw" an RPG and many, many more weapons the first time I saw the video. I was numb. I explored it further, and found out what actually happened later. I wanted the video to challenge that cognitive bias that every young Iraqi male is an insurgent.
3. I instructed there to be an Orwell quote, description of the journalists, and some general context. Assange came up with "Collateral Murder," with my approval. It literally means "unintentional murder."
4. Public Relations is an area WikiLeaks needed some desperate help in, since the only people who had heard of them before were people in the hacker, journalist, and intelligence communities.
5. Video personally pissed off Assange, and he wanted to "get out of exile."

PROSECUTION EXHIBIT H for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE OF PAGES

On 5/20/10 1:02 AM, Eric Schmiedl wrote:

Cool. Why all the PR spin over "collateral murder," when releasing it straight like previous leaks might have ended up winning more controversy?

On 5/19/10 5:50 PM, Bradley Manning wrote:

I was the source of the 12 JUL 07 video from the Apache Weapons Team, which killed the two journalists and injured two kids.

=L

On 5/20/10 12:46 AM, Eric Schmiedl wrote:

Yeah, I am.

On 5/19/10 5:46 PM, Bradley Manning wrote:

Are you familiar with WikiLeaks?

--
v/r

Manning, Bradley E.

On 5/20/10 12:41 AM, Eric Schmiedl wrote:

pass

On 5/19/10 5:41 PM, Bradley Manning wrote:

Test

On 5/20/10 12:37 AM, Eric Schmiedl wrote:

Here you go. Enjoy!

On 5/19/10 5:36 PM, Bradley Manning wrote:

Hey Eric,

It's been a little while since we last spoke. I was hoping I could get your OpenPGP info somehow... If you use it.

--
v/r

Manning, Bradley E.

Re: Hello Again

--
v/r

Manning, Bradley E.

--
v/r

Manning, Bradley E.

Items of Historical Significance for Two Wars:

Iraq and Afghanistan Significant Activities (SIGACTs) between 0000 on 01 JAN 2004 and 2359 on 31 DEC 2009 (Iraq local time, and Afghanistan local time)

CSV extracts are from the Department of Defense (DoD) Combined Information and Data Exchange (CIDNE) Database.

It's already been sanitized of any source identifying information.

You might need to sit on this information, perhaps 90-180 days, to figure out how best to release such a large amount of data, and to protect source.

This is possibly one of the more significant documents of our time, removing the fog of war, and revealing the true nature of 21st century asymmetric warfare.

Have a good day.

02

PROSECUTION EXHIBIT 15 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE OF PAGES

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

07 Jan 2010

(U) MARFOREUR G-2 TRIP REPORT¹

(U) Traveler: Staff Sergeant Matthew Hosburgh

(U) Purpose: Chaos Communication Congress 26C3 Here Be Dragons Conference

(U) Dates: 26–30 December 2009

(U) Location: Berlin, Germany

(U) **Executive Summary.** The Chaos Communication Congress conference is an annual event that attracts hackers, security researchers, computer hobbyists and malicious computer users. This year's conference marked the 26th year anniversary of the congress. The conference title was *Here Be Dragons* which is a reference to medieval times where explorers would put dragons or other serpents to mark dangerous or uncharted territories—an attempt to explain the conference's purpose in exposing 'uncharted territories' in computer, phone, and other systems. The conference began on 27 December 2009 and lasted until 30 December 2009. There were some good talks about security and some rather alarming developments in the 'uncharted territory.' A majority of the security discussions were in German which prevented attendance because of the language barrier; however, a large amount of the discussions were in English and catered to the international audience. I personally attended the following talks: Lightning Talks—Day 1; Why Net Neutrality Matters?; WikiLeaks Release 1.0; Exposing Crypto Bugs through reverse engineering; Tor and censorship: lessons learned; SCCP hacking, attacking the SS7 & SIGTRAN applications on step further and mapping the phone system; DDoS / botnet mitigation & hosting online communities; Using OpenBSC for fuzzing of GSM handsets; "Yes We Can't!"—on kleptography and cryptovirology; Black Ops of PKI. A detailed explanation, assessment and countermeasure (if applicable) can be found below.

1. (U) **Lightning Talks – Day 1.** Lightning Talks were a two hour forum where basically members of the hacking community could present a topic or announce an event for approximately four minutes. During this talk, there were

¹ **MARFOREUR AC/S G-2 Comment:** This paper has been declassified on 05 March 2012 in accordance with the procedures set forth in DoD Instruction 5200.1-R (Information Security Program; January 1997). Prior to declassification, this paper was reviewed by the MARFOREUR AC/S G-2 (Senior Intelligence Officer), MARFOREUR AC/S G-6 (Senior Communications Officer/Chief Information Officer), USEUCOM J2 (Cyber Intelligence Division), USEUCOM Foreign Disclosure Officer, and USEUCOM SSO (INFOSEC Branch), all of whom concurred that the information contained herein does not exceed a level of UNCLASSIFIED//FOR OFFICIAL USE ONLY. The paper's author, SSgt Matthew Hosburgh, was discharged from the United States Marine Corps in June 2010 and therefore was not available to participate in this declassification review.

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

PROSECUTION EXHIBIT 43 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE OF PAGES

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

presentations on TV-Be-Gone (a universal remote that can turn off television sets from a distance), and a few other projects that were not of much significance.

- a. (U) Analysis: This forum seemed vary inert. There was also a lack of speakers for day one as the Internet for the conference center was down and a lot of the presentations were stored on a website on the Internet.
b. (U) Countermeasure: N/A
2. (U) Why Net Neutrality Matters? Net neutrality is fast becoming a hot topic in the information technology world. Essentially, this talk presented what it is a way for an ISP companies to more tightly regulate levels of service to the user. This could be in the form of making users pay for exactly what they need on the Internet. For example, an ISP could provide a customer with three packages to choose from, say 1 – 3. Package 1 could cost \$30 per month and only allow access to Google searching and news websites. Package 2 could allow more access for \$40 per month including email, web browsing, and access to banking sites. Package 3 could be the “premium package” as it would allow access to music, YouTube and other media sites (to include packages 1 – 2). The ISPs would be able to regulate the internet content and not just bandwidth. This is the core issue: limiting access to content and not bandwidth. The talk made the case the Internet should be kept open and free. Jeremie Zimmerman was the presenter (a French citizen) and he said his organization had been lobbying the French politicians to keep the Internet open. His plea to everyone at the conference was to lobby in our respective countries to keep the Internet the way it is today.
 - a. -(S//NF)-(U//FOUO) Analysis: Keeping the Internet neutral has its benefits. It allows the free exchange of ideas which promotes global communications. Basically, the Internet is the same no matter where one is in the world (relatively speaking). Taking the openness out of the Internet would hinder global communications and business. On the flipside, the Internet, as it stands today, is a playground for malicious users (creating viruses, cyber fraud, child pornography, and other crimes). Further, the Internet is an essential communication tool for terrorists. Terrorists cells can use the Internet to obscure their traffic, as well as, other tools to encrypt, hide and send messages. By filtering the Internet, this problem may be minimized, but at the cost of lost revenue and freedom of speech.
b. (U) Countermeasure: N/A
3. (U) WikiLeaks Release 1.0. Wikileaks.org, is a publicly accessible Internet Website where individuals can contact with leaked information and have it published to the public anonymously without fear of being held legally liable. The information that can be leaked includes, but is not limited to, classified information, trade secrets, corporate information, personally identifiable information, and even operational data. The goal is to promote “open-ness” and

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

to ensure the public is "well informed" to what's really going on. The founders of WikiLeaks claim that they have not had any of their sources compromised or uncovered. One of the most alarming pieces of the talk was that WikiLeaks was seeking to obtain "off shore" storage and data processing of their site so that they would not be bound to U.S. law. This concept is similar to that of the proverbial "Swiss bank account."

- a. ~~(S//NF)~~ (U//FOUO) **Analysis.** WikiLeaks represents a potential force protection, counterintelligence, operational security (OPSEC), and information security (INFOSEC) threat to MARFOREUR/AF. The intentional or unintentional leaking and posting of US Marine Corps sensitive or classified information to WikiLeaks.org poses a large threat not only from the external disclosure, but from the insider. The insider would be able to easily leak information without fear of any direct, individual, repercussions. Further, when the off-shore storage is implemented, WikiLeaks will have more latitude to distribute and publish leaked information as it will not be bound by U.S. law.
 - b. **(FOUO) Countermeasure:** For MARFOREUR/AF, ensure that employees are given annual security training. Remind cleared individuals of their agreement to safeguard and not disclose classified or sensitive information. Enforce document accountability. Ensure that classified information that is no longer needed is properly disposed of. Recommend implementing a control to ensure that whoever prints, the document and user is logged for all systems (unclass - SCI). Enforce the secure print feature for the printers in the hallway, that is, where uncleared individuals may be in contact with the printers.
4. (U) **Exposing Crypto Bugs through reverse engineering.** This talk was given by Philippe Oechslin of Objectif Securite. He is also a French citizen. His talk was aimed at explaining how poor coding of programs could be a way to attack a system vice trying to break the encryption algorithm. Essentially, exploiting bugs to break-in/manipulate a device or system vice trying to exploit the encryption algorithm, such as AES or 3DES. The devices he demo'd were the MXI Stealth (a FIPS 142-3 level 2 certified USB flash drive), the EISST E-Capsule (an electronic safe for data), and the Data Becker Private Safe (another electronic safe). During his demo, he showed how he could break-in to the devices, by reverse engineering the code using publicly available Hex Editors and commercial tools. He used the poorly written code to obtain access to the devices.
- a. ~~(S//NF)~~ (U//FOUO) **Analysis.** Based on the demonstration, standard crypto algorithms, such as, AES and 3DES are very secure if implemented correctly. They will thwart any current type of brute force attack. However, if the programmer does not implement the crypto correctly, the device or program can be exploited or access can be obtained. The crypto

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

will remain unbroken, but the device or software can be broken because of poor implementation and reverse engineering.

- b. ~~(S//NF)~~ (U//FOUO) **Countermeasure.** Ensure that USB devices, that are relied on to provide a degree of security using crypto, are certified by the NSA or other agency to ensure that they are indeed secure and free from being reverse engineered. Simply buying a "secure USB" device from the PX is not an option if it not approved. Guard the keys to decrypt the device like a password and do not write them down. Use complex passphrases to secure the device and not an easily guessable word or phrase.

5. (U) **Tor and censorship: lessons learned.** Tor is an acronym for the "The Onion Router." It is a network spread across the globe and its aim is to provide anonymity and obscurity to its users. There are seven "root" servers that are maintained by staff members of tor and other relay networks hubs that users can setup to host an instance of Tor at their location. Tor is becoming quite popular today among many censored users, for example: China and Iran. Because China and Iran block and filter content, Tor is used to circumvent these restrictions. Tor is further becoming more of a hard-to-pin-down anonymizer. Roger Dingledine was the speaker. He gave the current state of Tor in the world and how it was being utilized. Even after China attempted to block Tor, the network evolved as is still able to function despite the blockage. An alarming statement made by one of his colleagues was that "we" "should get jobs at Cisco, Symantec and other security companies to find out what their intentions are for building these security appliances (firewalls, IDS, etc) and leak them to WikiLeaks." His colleague blamed the security vendors for making it easy for governments to censor its people and thus the need to find out why and how they were going to develop the next device to make filtering easier for an organization. He further went on to say that knowing why and how they are filtering will allow "the community" to respond by catering security appliances toward organizations (businesses) and not governments for censorship.

- a. ~~(S//NF)~~ (U//FOUO) **Analysis.** Tor is an effective tool that provides browser anonymity and obscurity on the Internet. It is free software available to the world. The threat it poses is that it makes it very difficult to know where certain traffic is coming from. For example, a malicious attacker could use it to obscure his or her IP address. MARFOREUR/AF's systems could be attacked by China and we would not know where they are coming from. The threat posed by this is not necessarily an insider one, it is primarily an outside threat. It would make it very difficult to monitor traffic of an individual / organization utilizing Tor.
- b. ~~(C)~~ (U//FOUO) **Countermeasure.** At this point, there is not much in the way of defense as the "standard" filtering of Tor traffic can be circumvented by way of using a relay circuit within the Tor network.

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Educate the users and the IA personnel on the power of Tor to hide where attacks may be coming from.

6. (U) **SCCP hacking, attacking the SS7 & SIGTRAN applications on step further and mapping the phone system.** In this talk, Philippe Langolis discussed the current state of the phone system. He said, "SS7 is like TCP/IP in the 1990s. It used to be quite a secure network because nobody outside the organizations (here, the mobile operators and telecom companies) were connected to it. Now it's getting interconnected to new actors which are not that trustworthy. He further went on to say that the Blue Box (used to generate tones which can access the "supervisory" function of the phone system. From there, additional tones can be used to generate desired effects) is making a come back. There's a world beyond pure SS7: the phone system applications themselves and most notably what transforms phone numbers into telecom addresses (also known as Point Codes, DPCs and OPCs; Subsystem Numbers, SSNs and other various fun.), and that's called Global Title Translation. Few people actually realize that the numbers they are punching on their phone are actually the same digits that are used for this critical translation function, and translate these into the mythical DPCs, SSNs and IMSIs. More and more data is now going through the phone network, creating more entry point for regular attacks to happen: injections, overflow, DoS by overloading capacities. The mobile part is opening up, thanks to involuntary support from Motorola, Apple and Android."
 - a. (U) **Analysis.** The attack surface for GSM is increasing daily. With more entry points, the technology is at the tip of the security nightmare iceberg. More security problems will ensue in the next few years.
 - b. (U) **Countermeasure.** N/A.
7. (U) **DDoS / botnet mitigation & hosting online communities.** This talk discussed the "business" of running an online community, such as, a social network, newsgroup, etc. The discuss honed in on what needs to happen while experiencing a Denial of Service (DoS) attack. Essentially, the speaker stressed the need to have a good relationship with the ISP or webhosting service incase something out of the ordinary should happen.
 - a. (U) **Analysis.** This discussion was relatively inert; however, it does go to show that the sophistication of some of the "underground" online communities are looking at hosting as more of a business—in such to keep their communities up incase of a disaster or attack.
 - b. (U) **Countermeasure.** N/A.
8. (U) **Using OpenBSC for fuzzing of GSM handsets.** More tools are available to attackers looking to exploiting the GSM network. This discussion painted the picture as to the current state of the GSM attack surface. The GSM protocol stack

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

-S E C R E T // N O F O R M -
UNCLASSIFIED//FOR OFFICIAL USE ONLY

is a communications protocol stack like any other. There are many layers of protocols, headers, TLV's, length fields that can "accidentally" be longer or shorter than the actual content. There are timers and state machines. Wrong messages can trigger invalid state transitions. This protocol stack inside the telephone is implemented in C language on the baseband processor on a real-time operating system without any memory protection. This flaw means that the attack surface is increased; especially, because of OpenBSC. OpenBSC is a tool that is freely available that can be used for GSM protocol hacking.

- a. ~~(S//NF)~~ (U//FOUO) **Analysis.** GSM networks have, for the most part, been off limits for attackers (phreakers) historically speaking. With the release of these freely available GSM protocol tools (OpenBSC), the avenues for attacking GSM has greatly increased. This could be a precursor for a security nightmare on the GSM network. Expect to see more attacks on the GSM network in the near future.
- b. ~~(S//NF)~~ (U//FOUO) **Countermeasure.** Enforcing OPSEC and INFOSEC training is a must. As the GSM network can be attacked by anyone not only for eavesdropping, but for denying service. Consider using secure Iridium phones whenever practical.
9. (U) "Yes We Can't!" – on kleptography and cryptovirology. What is kleptography and cryptovirology? Kleptography (the art of employing public key cryptography maliciously as part of a malware attack, such as in ransomware) and the related cryptovirology (the art of embedding cryptographic Trojans inside tamper-proof cryptosystems). During this talk Dr. Moti Yung discussed some of the realities of these threats. He didn't go into detail of how to employ the two, but he did underscore the security threat that the two malicious attacks can present. This is an instance where something that was developed to bring security and peace of mind has been manipulated into something that an attacker can use to blackmail and/or attack without much effort.
 - c. (U) **Analysis.** These two attacks are very serious and can be difficult to attack and remedy. Traditional virus signatures will have a hard time recognizing cryptovirology. Phishing attacks, especially brought on by poor OPSEC and PII practices, can make this attack easier to be conducted.
 - d. ~~(C)~~ (U//FOUO) **Countermeasure.** Ensure that users are briefed about phishing and spear fishing attacks. Keep virus definitions up-to-date and ensure that email signatures are being utilized within MARFOREUR/AF. At home, do not open email that you do not know the sender. Be weary, if a deal sounds too good to be true, it most likely is.
10. (U) **Black Ops of PKI.** This talk was given by Dan Kaminsky. He is a penetration tester for a security company in the US. He made the case for the insecurity of PKI on the Internet. Mainly, because of the lack of trusted

-S E C R E T // N O F O R M -
UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

certificate authorities—it is far too easy to obtain a “valid” certificate. Further, he explained some of the common ways to masquerade as a valid certificate in several different web browsers (Internet Explorer being one). He went on to praise the DoD for having a working PKI system. For the open Internet, he said he had hope in Secure DNS in hopefully curbing the number of invalid/unauthorized certificate authorities. Basically, making it harder to obtain a certificate and making PKI more secure.

- a. (U) **Analysis.** Secure DNS will help with the issue of certificate authority on the Internet. It is scheduled to be released within about six months. The current state is that PKI on the Internet should not be considered a means to identify an entity or user is who they say they are. The DoD should continue to implement and secure the PKI CAs to ensure the infrastructure validity.
- b. (U) **Countermeasure.** Ensure that users at MARFOREUR/AF are aware that the PKI on the Internet is not the same as PKI within the DoD. It is not secure, so do not trust it like you would at work. Not to say it cannot be trusted, it just needs to be scrutinized more.

(U) **Conclusion.** The Chaos Communication Congress 26C3 Here Be Dragons conference was a good security conference to attend. It explored the “out-of-band” security issues faced by systems currently employed by the world and specifically, the DoD (MARFOEUR/AF). The conference provided a good means to observe the hacker community in Europe. The talks provided interesting and thought provoking security discussions which can be used to provide awareness at MARFOREUR/AF. From what I gathered, there were no impending direct attacks (hacks) on US Persons or MARFOREUR at the conference.

M. J. HOSBURGH

~~SECRET//NOFORN~~
UNCLASSIFIED//FOR OFFICIAL USE ONLY

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**



Army Counterintelligence Center
Special Report

[ACIC Home](#)

(U) Wikileaks.org—An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?

NGIC-2381-0617-08

Information Cutoff Date: 28 February 2008

Publication Date: 18 March 2008

National Security Information

Unauthorized Disclosure Subject to Criminal Sanctions

Derived from: Multiple sources

Declassify on: Source documents marked 25X1

Date of source: 20060725

This Counterintelligence Analysis Report is published under the auspices of the Department of Defense Intelligence Analysis Program (DIAP).

Prepared by:

Michael D. Horvath

Cyber Counterintelligence Assessments Branch

Army Counterintelligence Center

External Coordination: National Ground Intelligence Center [\[1\]](#)

This product responds to HQ, Department of Army, production requirement C764-97-0005.

ACIC Product Identification Number is RB08-0617.

[\[Back to Table of Contents\]](#)

(U) Purpose

(U) This special report assesses the counterintelligence threat posed to the US Army by the Wikileaks.org Web site.

[\[Back to Table of Contents\]](#)

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)** *Page 1 of 32* *02*

PROSECUTION EXHIBIT *45* for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE _____ OF _____ PAGES

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(U) Executive Summary

(S//NF) Wikileaks.org, a publicly accessible Internet Web site, represents a potential force protection, counterintelligence, operational security (OPSEC), and information security (INFOSEC) threat to the US Army. The intentional or unintentional leaking and posting of US Army sensitive or classified information to Wikileaks.org could result in increased threats to DoD personnel, equipment, facilities, or installations. The leakage of sensitive and classified DoD information also calls attention to the insider threat, when a person or persons motivated by a particular cause or issue unwittingly provides information to domestic or foreign personnel or organizations to be published by the news media or on the Internet. Such information could be of value to foreign intelligence and security services (FISS), foreign military forces, foreign insurgents, and foreign terrorist groups for collecting information or for planning attacks against US force, both within the United States and abroad.

(S//NF) The possibility that a current employee or mole within DoD or elsewhere in the US government is providing sensitive information or classified information to Wikileaks.org cannot be ruled out. Wikileaks.org claims that the "leakers" or "whistleblowers" of sensitive or classified DoD documents are former US government employees. These claims are highly suspect, however, since Wikileaks.org states that the anonymity and protection of the leakers or whistleblowers is one of its primary goals. Referencing of leakers using codenames and providing incorrect employment information, employment status, and other contradictory information by Wikileaks.org are most likely rudimentary OPSEC measures designed to protect the identity of the current or former insiders who leaked the information. On the other hand, one cannot rule out the possibility that some of the contradictions in describing leakers could be inadvertent OPSEC errors by the authors, contributors, or Wikileaks.org staff personnel with limited experience in protecting the identity of their sources.

(U) The stated intent of the Wikileaks.org Web site is to expose unethical practices, illegal behavior, and wrongdoing within corrupt corporations and oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa, and the Middle East. To do so, the developers of the Wikileaks.org Web site want to provide a secure forum to where leakers, contributors, or whistleblowers from any country can anonymously post or send documentation and other information that exposes corruption or wrongdoing by governments or corporations. The developers believe that the disclosure of sensitive or classified information involving a foreign government or corporation will eventually result in the increased accountability of a democratic, oppressive, or corrupt the government to its citizens.^[2]

(S//NF) Anyone can post information to the Wikileaks.org Web site, and there is no editorial review or oversight to verify the accuracy of any information posted to the Web site. Persons accessing the Web site can form their own opinions regarding the accuracy of the information posted, and they are allowed to post comments. This raises the possibility that the Wikileaks.org Web site could be used to post fabricated information; to post misinformation, disinformation, and propaganda; or to conduct perception management and influence operations designed to convey a negative message to those who view or retrieve information from the Web site.^[3]

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)** Page 2 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(U) Diverse views exist among private persons, legal experts, advocates for open government and accountability, law enforcement, and government officials in the United States and other countries on the stated goals of WikiLeaks.org. Some contend that the leaking and posting of information on WikiLeaks.org is constitutionally protected free speech, supports open society and open government initiatives, and serves the greater public good in such a manner that outweighs any illegal acts that arise from the posting of sensitive or classified government or business information. Others believe that the Web site or persons associated with WikiLeaks.org will face legal challenges in some countries over privacy issues, revealing sensitive or classified government information, or civil lawsuits for posting information that is wrong, false, slanderous, libelous, or malicious in nature. For example, the WikiLeaks.org Web site in the United States was shutdown on 14 February 2008 for 2 weeks by court order over the publishing of sensitive documents in a case involving charges of money laundering, grand larceny, and tax evasion by the Julius Bare Bank in the Cayman Islands and Switzerland. The court case against WikiLeaks.org was dropped by Julius Bare Bank, the US court order was lifted and the Web site was restored in the United States. Efforts by some domestic and foreign personnel and organizations to discredit the WikiLeaks.org Web site include allegations that it unwittingly allows the posting of uncorroborated information, serves as an instrument of propaganda, and is a front organization of the US Central Intelligence Agency (CIA). [4]

(S//NF) The governments of China, Israel, North Korea, Russia, Thailand, Zimbabwe, and several other countries have blocked access to WikiLeaks.org-type Web sites, claimed they have the right to investigate and prosecute WikiLeaks.org and associated whistleblowers, or insisted they remove false, sensitive, or classified government information, propaganda, or malicious content from the Internet. The governments of China, Israel, and Russia claim the right to remove objectionable content from, block access to, and investigate crimes related to the posting of documents or comments to Web sites such as WikiLeaks.org. The governments of these countries most likely have the technical skills to take such action should they choose to do so. [5]

(S//NF) WikiLeaks.org uses trust as a center of gravity by assuring insiders, leakers, and whistleblowers who pass information to WikiLeaks.org personnel or who post information to the Web site that they will remain anonymous. The identification, exposure, or termination of employment of or legal actions against current or former insiders, leakers, or whistleblowers could damage or destroy this center of gravity and deter others from using WikiLeaks.org to make such information public.

[\[Back to Table of Contents\]](#)

(U) Key Judgments

- (S//NF) WikiLeaks.org represents a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army.
- (S//NF) Recent unauthorized release of DoD sensitive and classified documents provide FISS, foreign terrorist groups, insurgents, and other foreign adversaries with potentially actionable information for targeting US forces.
- (S//NF) The possibility that current employees or moles within DoD or elsewhere in the US government are providing sensitive or classified information to WikiLeaks.org cannot

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**Page 3 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

be ruled out. The claim made by WikiLeaks.org that former US government employees leaked sensitive and classified information is highly suspect, however, since WikiLeaks.org states that the anonymity of the whistleblowers or leakers is one of its primary goals.

- (U//FOUO) The WikiLeaks.org Web site could be used to post fabricated information, misinformation, disinformation, or propaganda and could be used in perception management and influence operations to convey a positive or negative message to specific target audiences that view or retrieve information from the Web site.
 - (U//FOUO) Several countries have blocked access to the WikiLeaks.org Web site and claim the right to investigate and prosecute WikiLeaks.org members and whistleblowers or to block access to or remove false, sensitive, or classified government information, propaganda, or other malicious content from the Internet.
 - (U//FOUO) WikiLeaks.org most likely has other DoD sensitive and classified information in its possession and will continue to post the information to the WikiLeaks.org Web site.
 - (U//FOUO) Web sites such as WikiLeaks.org use trust as a center of gravity by protecting the anonymity and identity of the insiders, leakers, or whistleblowers. The identification, exposure, termination of employment, criminal prosecution, legal action against current or former insiders, leakers, or whistleblowers could potentially damage or destroy this center of gravity and deter others considering similar actions from using the WikiLeaks.org Web site.
-

(U) Table of Contents

- (U) Purpose
- (U) Executive Summary
- (U) Key Judgments
- (U) Background
- (U) Discussion
- (U) Intelligence Gaps
- (U) Conclusions
- (U) Point of Contact
- (U) References
- (U) Appendix A: Glossary
- (U) Appendix B: Methodology Used by Authors for Analysis of Leaked Tables of Equipment for US Forces in Iraq and Afghanistan

(U) Tables

- (U) Table 1. Abbreviated Listing of the Iraq Transition Team (UIC - M94216) Table of Equipment (TOE)
- (U) Table 2. Descriptive Entry of the File and How it is Catalogued by WikiLeaks.org for the NGIC Report Entitled "(U) Complex Environments: Battle of Fallujah I, April 2004" [NGIC-1127-7138-06] posted on its Web site

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)** Page 4 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(U) Figures

- (U) Figure 1. M33A1 Bulk CS Chemical Dispenser
 - (S//NF) Figure 2. Map from Page 4 of NGIC Report Entitled "(U) Complex Environments: Battle of Fallujah I, April 2004" As Published in a WikiLeaks.org Article.
-

[\[Back to Table of Contents\]](#)

(U) Background

(U//FOUO) WikiLeaks.org was founded by Chinese dissidents, journalists, mathematicians, and technologists from the United States, China, Taiwan, Europe, Australia, and South Africa. Its Web site became operational in early 2007. The advisory board for WikiLeaks.org includes journalists, cryptographers, a "former US intelligence analyst," and expatriates from Chinese, Russian, and Tibetan refugee communities. The ACIC does not have any information to associate or link the "former US intelligence analyst" on the WikiLeaks.org advisory board with the leakage of sensitive or classified DoD documents posted to the Web site.[\[6\]](#)

(U) WikiLeaks.org claims to have developed an uncensorable version of the publicly available Wikipedia interface that is intended for mass leakage of sensitive documents that expose wrongdoing and for allowing users to comment on the documents posted to the Web site. Through its Web site, WikiLeaks.org encourages large-scale anonymous leaking and posting of sensitive and confidential government and business documents on the Internet. WikiLeaks.org claims to have received more than 1.2 million documents from dissident communities and anonymous sources throughout the world. If true, additional articles involving sensitive or classified DoD will most likely be posted to the WikiLeaks.org Web site in the future.[\[7\]](#)

(S//NF) WikiLeaks.org uses its own coded software combined with Wiki, MediaWiki, OpenSSL, FreeNet, TOR, and PGP to make it difficult for foreign governments, FISS, law enforcement agencies, and foreign businesses to determine where a leaked document originated from and who was responsible for leaking the document. The goal of WikiLeaks.org is to ensure that leaked information is distributed across many jurisdictions, organizations, and individual users because once a leaked document is placed on the Internet it is extremely difficult to remove the document entirely.[\[8\]](#)

(S//NF) The obscurification technology[\[9\]](#) used by WikiLeaks.org has exploitable vulnerabilities. Organizations with properly trained cyber technicians, the proper equipment, and the proper technical software could most likely conduct computer network exploitation (CNE) operations or use cyber tradecraft to obtain access to WikiLeaks.org's Web site, information systems, or networks that may assist in identifying those persons supplying the data and the means by which they transmitted the data to WikiLeaks.org. Forensic analysis of DoD unclassified and classified networks may reveal the location of the information systems used to download the leaked documents. The metadata, MD5 hash marks, and other unique identifying information within digital documents may assist in identifying the parties responsible for leaking the information. In

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**Page 5 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

addition, patterns involving the types of leaked information, classification levels of the leaked information, development of psychological profiles, and inadvertent attribution of an insider through poor OPSEC could also assist in the identification of insiders.

(U) WikiLeaks.org supports the US Supreme Court ruling regarding the unauthorized release of the Pentagon Papers by Daniel Ellsberg, which stated that "only a free and unrestrained press can effectively expose deception in government." The WikiLeaks.org Web site further states the following:

"We aim for maximum political impact. We believe that transparency in government activities leads to reduced corruption, better government, and stronger democracies. All governments can benefit from increased scrutiny by the world community, as well as their own people. We believe this scrutiny requires information. Historically that information has been costly—in terms of human life and human rights. But with technological advances—the Internet, and cryptography—the risks of conveying important information can be lowered."[10]

(U) The OPSEC measures used in the submission of leaked information to WikiLeaks using the Internet are designed to protect the identity and personal security of the persons or entities sending or posting information to the Web site. WikiLeaks.org claims that any attempt at trace routing of IP addresses, MAC addresses, and other identifying information of a home computer submissions (as opposed to cyber café submissions) through WikiLeaks.org's Internet submission system would require a knowledge of information available only to WikiLeaks.org programmers and to a rights organization serving the electronic community, or would require specialized ubiquitous traffic analysis of Internet messages and routing systems. Nevertheless, it remains technically feasible for FISS, law enforcement organizations, and foreign businesses that have the motivation, intentions, capability, and opportunity to gain online access or physical access to WikiLeaks.org information systems to identify and trace whistleblowers through cyber investigations, advanced cyber tools, and forensics.[11]

(U) Another method of posting leaked information to the Web site anonymously is for leakers to use postal mail to send the information to volunteers in various countries who have agreed to receive encrypted CDs and DVDs from leakers. These volunteers then forward the information to designated personnel, who then upload the data on the CDs and DVDs to the WikiLeaks.org Web servers. To protect or mask the sender, leakers can take OPSEC measures such as using WikiLeaks.org encryption protocols when writing CDs and DVDs; using gloves while wrapping, taping, handling, and mailing packages; and not including a return address or including a fake return address on packages containing leaked information. Such measures are designed to protect the identity of the leakers and prevent FISS, law enforcement, and postal inspectors from intercepting the mail and decoding the information on the data storage devices in transit. WikiLeaks.org also claims that it is developing easy-to-use software to encrypt the CDs and DVDs. Use of such methods also protects facilitators or intermediaries from harm because they would not know the content of the encrypted submissions.[12]

(U) A WikiLeaks.org spokesperson stated in early January 2007 that about 22 persons are involved in the Open Society Initiative to make governments and corporations more accountable

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

to the citizens of the world. WikiLeaks intends to seek funding from individual persons and groups such as humanitarian organizations that fund sociopolitical activity intended to promote democracy and human rights around the world through open access to government and business information.[\[13\]](#)

(S//NF) Several foreign countries including China, Israel, North Korea, Russia, Vietnam, and Zimbabwe have denounced or blocked access to the WikiLeaks.org Web site to prevent citizens or adversaries from accessing sensitive information, embarrassing information, or alleged propaganda. The governments of China, Israel, and Russia have asserted that they have a right to remove from the Internet protected government information, disinformation, and propaganda that is intended to embarrass or make false allegations against their governments. China, Israel, North Korea, and Russia are assessed to have state-sponsored CNE, computer network attack (CNA), and cyber forensics capabilities that would most likely allow penetration or disrupt viewing of the WikiLeaks.org Web site. China, Israel, and Russia have used or are suspected of having used CNA to target terrorist or dissident Web sites that have posted objectionable material intended to embarrass, harm, or encourage terrorism or opposition to the government [\[14\]](#)

[\[Back to Table of Contents\]](#)

(U) Discussion

(U//FOUO) An insider could present a potential force protection, counterintelligence, OPSEC, or INFOSEC threat to the US Army through deliberate unauthorized release of official DoD documents and posting of sensitive or classified information to the Internet. Several recent postings to the WikiLeaks.org Web site in November 2007 of sensitive US Army information marked UNCLASSIFIED//FOR OFFICIAL USE ONLY and in December 2007 of US Army information classified SECRET//NOFORN highlight the insider threat to DoD. The actual perpetrators responsible for the unauthorized released of such documents could be subject to administrative action, nonjudicial punishment, or criminal charges and prosecution if they are identified.

(U) WikiLeaks.org Analysis of US Army Tables of Equipment in Iraq and Afghanistan from April 2007

(U) WikiLeaks.org specifically cited 2,000 pages of leaked US Army documents with information on the Tables of Equipment (TOEs) for US and Coalition forces in Iraq and Afghanistan as a perfect example of the sort of information that would benefit from a global analysis. These documents provided information on the US forces, a description of equipment and total number of equipment that were assigned to actual military units assigned to US Central Command in April 2007. WikiLeaks.org staff members and various authors and contributors have written numerous news articles and posted the raw data in spreadsheets or Structured Query Language (SQL) data base so anyone can examine the information, conduct research, comment upon, discuss the various units, see the items of equipment, see what they do, and draw their own conclusions about the strategic, political, military, and human rights significance of the information.[\[15\]](#)

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(U//FOUO) *Table 1* below is an abbreviated sample of information contained in a leaked digital database document or spreadsheets available on the WikiLeaks.org Web site:

[\[Back to Table of Contents\]](#)

**(U) Table 1. Abbreviated Listing of the Iraq Transition Team (UIC - M94216)
Table of Equipment (TOE). [16]**

UIC	LIN	NSN	Item Name	PBIC	Type	DND	Qnty
M94216	72045Z	581001X111125	WARLOCK GREEN, ECM: GREEN EDO CO	V	TPE	N	15
M94216	72113Z	581001X111126	WARLOCK RED, ECM: RED EDO COMM &	T	TPE	N	2
M94216	72113Z	581001X111126	WARLOCK RED, ECM: RED EDO COMM &	V	TPE	N	13
M94216	B67766	1.24001E+12	BINOCULA MOD CN M22	N	TPE	N	9
M94216	E63317	6.60501E+12	COMPAS MAGNETIC UNMFTD	P	TPE	N	3
M94216	J03261	5.85501E+12	ILLUMI INFR AN/PEQ-2A	P	TPE	N	6
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	4
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	49
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	8
M94216	J85705	8.47002E+12	INSERTS,ENHANCED SM	N	TPE	N	49
M94216	L91975	1.005E+12	MG 50 M2 HB FL GD/VEH	P	TPE	N	3
M94216	L92352	1.00501E+12	MACH GUN 7.62MM M240	N	TPE	N	2
M94216	M09009	1.00501E+12	MACH GUN 5.56MM M249	P	TPE	N	3
M94216	M74823	1.01001E+12	MT MACH GUN MK64 MOD9	T	TPE	N	1
M94216	M75577	1.005E+12	MT TPD MG CAL .50 M3	P	TPE	N	1
M94216	M92841	1.00501E+12	MACH GUN 7.62MM M240B	N	TPE	N	2
M94216	M92841	1.00501E+12	MACH GUN 7.62MM M240B	T	TPE	N	2
M94216	N05482	5.85501E+12	NIGHT VIS G AN/PVS-7B	P	TPE	N	8
M94216	T92446	2.32001E+12	TRK UTIL HMMWV M1114	T	TPE	N	1
M94216	W95537	2.33001E+12	TRL CGO 3/4T M101 2WH	T	TPE	N	3
M94216	YF2014	232001C043031	HMMWV M1114: W/ OFKS	T	TPE	N	2
M94216	YF2049	2.32001E+12	TRUCK,UTILITY-(M1116)	T	TPE	N	1

Legend:

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**Page 8 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

UIC – Unit Identification Code, a six-character, alphanumeric code that uniquely identifies each Active, Reserve, and National Guard unit of the US Armed Forces.

LIN – Line Item Number for equipment.

NSN – NATO Stock Number, a standardized stock identification number for supplies and equipment within the North Atlantic Treaty Organization.

Item Name - Brief description of the equipment.

PBIC – Property Book Identification Code, which categorizes the type of property listed into one of 10 categories.

Type (of equipment):

TPE – Theater Provided Equipment; specific equipment that is provided by the Theater of Operations such as CENTCOM to perform the mission based on the unique operating environment

LT – Long Term Training; equipment need for long term training or deployment.

APS – Army Prepositioned Stock; equipment drawn by a unit that is already prepositioned in the Theater of Operations.

DND – Do Not Deploy; this field is a Yes/No column that lists equipment that remains at the home station and is not deployed with the unit when sent overseas.

OH Qty – On-hand Quantity is the number of item of equipment that is currently available to the unit; it does not necessarily represent the actual required number needed by the unit to be fully mission capable [17]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~(S/NF)~~ The foreign staff writer for Wikileaks.org, Julian Assange, wrote several news articles, coauthored other articles, and developed an interactive data base for the leaked documents. In addition, other Wikileaks.org writers and various writers for other media publications wrote separate news articles based on the leaked information posted to the Web site. Assange and his coauthors claim that the 2,000 pages of leaked US military information provides unit names, organizational structure, and tables of equipment (TOEs) for the US Army in Iraq and Afghanistan. They also claimed that unidentified persons within the US government leaked the information to facilitate action by the US Congress to force the withdrawal of US troops by cutting off funding for the war.[18]

(U//FOUO) Assange and other Wikileaks.org writers purport that the leaked sensitive TOE information reveals the following:

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**Page 9 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

- Secretive US document exploitation centers.
- Detainee operations and alleged human rights violations.
- Information on the US State Department, US Air Force, US Navy and US Marines units, Iraqi police and coalition forces from Poland, Denmark, Ukraine, Latvia, Slovakia, Romania, Armenia, Kazakhstan, and El Salvador serving in Iraq and Afghanistan.
- Nearly the entire order of battle for US forces in Iraq and Afghanistan as of April 2007.
- Alleged revelations that the US government violated the Chemical Weapons Convention in Iraq and Afghanistan.^[19]

(S//NF) WikiLeaks.org encouraged persons to comment on the leaked Army documents and explained how the catalogued information and cross-referenced databases could be used by other researchers or journalists to prepare reports or assessments. According to WikiLeaks.org, the information posted can be used to prepare objective new reports. Conversely, this same information could be manipulated to prepare biased news reports or be used for conducting propaganda, disinformation, misinformation, perception management, or influence operations against the US Army by a variety of domestic and foreign actors.^[20]

(U) Assange and other WikiLeaks.org writers developed and applied a specific methodology for examining and analyzing the leaked TOE information, a methodology they then placed online to assist others in conducting their own research. See *Appendix B*. They also provided links to associated online reference material. The methodology used by Assange and other authors for the analysis of leaked tables of equipment for US Forces in Iraq and Afghanistan both a SQLite database is described in *Appendix B*.

(S//NF) The TOEs for US Army units deployed to Afghanistan and Iraq in April 2007 provide a wealth of information that could be used by FISS, foreign terrorist groups, and Iraqi insurgents to identify unit capabilities and vulnerabilities that could assist in conducting attacks against camps, convoys, and other targets. The information can also be compared with other publicly available databases to develop extensive order of battle files of vehicle types, communications and jamming equipment, information systems, and weapons systems, files that could be used to determine the capabilities, limitations, and vulnerabilities of the organic equipment assigned to military units. Such information could aid enemy forces in planning terrorist attacks, selecting the most effective type and emplacement of improvised explosive devices (IEDs), building triggering devices to defeat countermeasures organic to friendly units, and selecting the most effective direct and indirect weapons systems for conducting physical attacks against targets such as military units, convoys, and base camps.

(U) One WikiLeaks.org news article also discusses the use of IEDs by foreign terrorists and insurgent groups and claims that the IED threat has resulted in a shift in DoD funding priorities, similar to the Manhattan Project to develop atomic weapons in World War II, for current research, development and fielding of IED countermeasures through the Joint IED Defeat Organization. In addition, the author of the article attempts to provide a cost-to-benefit analysis of these IED tactics and countermeasures. The author claims that the leaked information reveals that 12,097 Warlock, Counter RCIED (Remote-controlled Improvised Explosive Device) Electronic Warfare (CREW), systems are in Iraq and that the purpose of the Warlock is to jam radio signals from devices such as mobile phones to prevent such signals from detonating IEDs.

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

The author claimed that 7,530 systems used in Iraq were purchased at a cost of \$1.1 billion. No claim was made regarding the cost of remaining 4,567 systems.

(S//NF) The author of the above-mentioned article incorrectly interprets the leaked data regarding the components and fielding of the Warlock system, resulting in unsupportable and faulty conclusions to allege war profiteering, price gouging and increased revenues by DoD contractors involved in counter-IED development efforts. This article provides an example of how the leaked TOE information can be manipulated and misinterpreted to produce inaccurate information for a news article.

(S//NF) The author of the article then argues that the US Army receives a poor return on its investment in counter-IEDs. The following excerpt from the article could be used by adversaries in potential propaganda or influence operations:

If we view IEDs as a rebel investment, to which the United States must pay dividends in defensive equipment costs, then every insurgent dollar spent has a return on investment of somewhere around a thousand fold. Significant price gouging by counter-IED defense contractors is evident. For comparison, each briefcase-sized "Warlock" IED jammer, of which is there is on average more than one per vehicle, is worth \$150,000; however, as can be seen by this analysis that is more costly than nearly every vehicle it was designed to protect. The "Warlock" producer, a DoD defense contractor [name redacted], predicts financial year 2007 will see a 400 percent total revenue increase over its 2003 levels.^[21]

(S//NF) Intelligence indicates that insurgents in Afghanistan have recovered several Warlock systems.^[22] It is possible that Warlock systems captured in Afghanistan were sent to Iran for reverse engineering and for use in developing countermeasures to Warlock.

(S//NF) Were a Warlock system successfully reversed engineered or countermeasures successfully developed by foreign terrorists, insurgents, or the Iranian government, US and Coalition forces would be at greater risk of RCIED attacks, especially those units equipped with Warlock systems similar to those that had been captured and exploited. It is also possible that any countermeasures developed to defeat the Warlock system would be provided to the Jaysh al-Mahdi (JAM) and other anti-US insurgent or terrorist groups operating in Iraq and Afghanistan. The TOEs could be used to identify and target specific units equipped with the same type of Warlock systems for which countermeasures had been developed.

(U) The WikiLeaks.org authors believe that the leaked documents list Army equipment held by the US Army, Marines, Air Force, Coalition, and possibly CIA units in Iraq and Afghanistan as of April 2007. The authors stated that the data only includes items registered with battle planning systems for logistics and appears to cover most valuable major end items of equipment. The data, according to the authors, does not include soldiers' combat pay, transportation, research and development, and home station costs of the soldiers, nor does it include most supplies, ammunition, and other disposable equipment and consumable items.^[23]

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(U) WikiLeaks.org staff personnel allegedly wrote a script or computer program to cross reference each item in the leaked document with NSNs gleaned from public US logistics equipment price catalogs from the Defense Logistics Agency (DLA). The authors claim that \$1.112 billion worth of US Army-managed military equipment in Afghanistan is listed in the leaked documents. The author believed the actual total value of the equipment to be several times higher.[\[24\]](#)

(U) The spreadsheets and list contains codes to identify military units, supply item codes, and other logistics data. The authors believed that the most useful data field for investigatory purposes was the NSN. The authors found several Internet sites that allow public searches of the NSNs, and this information was merged with the TOE into the SQL-generated database on the Web site. For example, the author specifically mentioned NSN catalogues that are publicly available on the Internet from the DLA.[\[25\]](#) The DLA Web site identifies many items on the spreadsheets and includes prices that were merged into the database and used to generate the estimate for the total value of the equipment.[\[26\]](#)

(U//FOUO) Julian Assange also stated in his news articles involving the TOE information that persons were welcome to assist in the following future actions and areas of research involving the equipment listings:

- A computer program would be written to expand the military unit abbreviations (for example, HHC—Headquarters and Headquarters Company) to make it easier for users to visually analyze entries in the database.
- Make further comments on military units in the list and their significance. The entries would be cross linked with available news sources.
- Make further comments on equipment items in the list and their significance.
- Expand and improve links and other information for US war-funding legislation and bills.
- Attempt to answer questions on specific issues with NSN codes. The authors stated that the NSNs are a 13-digit code. Of those 13 digits, 12 are numeric. The seventh is alphanumeric, and the publicly searchable NSN database seems to be able to locate items if they have a number in the seventh place, but, not if there is a letter in the seventh place. They ask the following questions: 1) What is the significance for this alphanumeric character in the seventh position? 2) What does a letter as opposed to a number signify? 3) Is there a more complete public database for NSN codes than the one given? 4) Are these alphanumeric NSNs Management Control Numbers as speculated?
- Create an interactive database browser.[\[27\]](#)

(U) Julian Assange and other WikiLeaks.org authors continually encourage other persons with an interest in the information to comment on their work or conduct their own research and publish the results on WikiLeaks.org.

(U) Alleged Violations of the Chemical Warfare Convention Treaty by US Military in Iraq and Afghanistan

(U) On 9 November 2007, WikiLeaks.org published an exclusive investigative report claiming that the United States "had almost certainly violated the Chemical Weapons Convention"

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(CWC), as originally drafted by the United Kingdom in 1997. The author, Julian Assange, claimed the deployment of CS (2-chlorobenzalmalononitrile also called Chlorobenzylidene Malononitrile) munitions and dispensing equipment and weapons capable of firing CS gas by the United States was a violation of the CWC. The author also claimed the United States had at least 2,386 low-grade chemical weapons deployed in Iraq and Afghanistan. These items also appeared in the 2,000-page listing of nearly one million items of US military equipment deployed in Iraq and leaked to WikiLeaks.org. The items are labeled under the military's own NATO supply classification for chemical weapons and equipment.^[28]

(U) Prior to the invasion of Iraq in 2003, the Defense Department released an official statement that President Bush had authorized US military forces to use riot control agents (RCAs) such as tear gas or CS gas. *See Figure 1.* The Defense Department stated that tear gas or CS gas, which was issued to US troops, would be used only to save civilian lives and in accordance with the CWC, as amended and ratified by the United States. Some chemical weapons experts in the United States and other countries expressed the belief that this 2003 authorization might violate the CWC treaty. These domestic and foreign critics expressed the belief that any battlefield use of tear gas would violate the CWC; offend crucial allies, including the United Kingdom and Australia. In addition, the critics claimed that the usage of CS would provide the Iraqi leader, Saddam Hussein, a pretext for using chemical weapons against the United States and coalition forces.^[29]

UNCLASSIFIED

M33A1 EMPLOYMENT DISPERSING A DRY CS SPRAY



(U) Figure 1. M33A1 Bulk CS Chemical Dispenser.

[\[Back to Table of Contents\]](#)

(U//FOUO) In the report published on WikiLeaks.org, the author claimed that any use of chemical weapons such as CS gas for military operations is illegal. The Chemical Weapons Convention of 1997, drafted by the United Kingdom declares "Each State Party undertakes not to use riot control agents as a method of warfare." It only grants permissible use to "law

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Page 13 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

enforcement including domestic riot control." The authors used this interpretation of the CWC drafted by the United Kingdom to make the allegation that the United States had violated the treaty. [30]

(U//FOUO) It must be noted, that US policy as stated in Executive Order No. 11850, 8 April 1975, *Renunciation of Certain Uses in War of Chemical Herbicides and Riot Control Agents*, renounced first use of herbicides in war (except for specified defensive uses) and first use of RCAs in war except for defensive military modes to save lives. In ratifying the CWC, the Senate wrote an amendment into its resolution approving the CWC that stated United States' interpretation of how RCAs might be used for specific defensive purposes, as specified by the 1975 Executive Order [31].

(U) Such varying interpretations reflect a deliberate ambiguity in the CWC, which states that "riot-control agents may not be used as a method of warfare." The original CWC and modified CWC approved by the US Senate, however, does not define this phrase "method of warfare." The actual version of the CWC passed by the US Senate was not considered by the authors of the report. The CWC ratified by the US Senate list exceptions in the usage of RCAs for US military forces that are not considered by the US government to be in violation of the CWC [32].

(U) In the same report, the authors claimed that the use of white phosphorus by the US military during the 2004 assault on Fallujah, Iraq, should also be considered a violation of the CWC. The authors noted, however, that the US Army claimed usage of white phosphorous as "a smoke screen" and "an incendiary" in the Fallujah operation, and that this usage is not technically covered by the CWC.

(U) Alleged Human Rights Violations Related to Joint Task Force-Guantanamo Standard Operating Procedures

(U//FOUO) Another example of leaked information posted to the WikiLeaks.org Web site on or about 7 November 2007 is an outdated copy of the Joint Task Force-Guantanamo, Camp Delta Standard Operating Procedures (SOP) marked as UNCLASSIFIED//FOUO, signed by MG Miller and dated 28 March 2003. A news article written by WikiLeaks.org staff writers, also posted on 7 November 2007, claims the SOP exposes systematic methods for preventing illegal combatants and detained prisoners incarcerated at Joint Task Force-Guantanamo facilities at Camp Delta from meeting with the International Red Cross, as well as the use of extreme psychological stress as a means of torture against detainees. The unauthorized release of the SOP has prompted authors posting to the WikiLeaks.org Web site to claim that the document proves the US Army was torturing and violating the human rights of detainees held at Guantanamo Bay. This SOP was also the subject of a lawsuit by international human rights groups and a domestic civil rights organization requesting the release of the document under the US Freedom of Information Act.[33]

(U) The author claimed that subsequent US military statements including a DoD spokesperson, to Reuters News Service and the *Miami Herald* confirm the veracity of the JTF SOP document. On Wednesday, 14 November 2007, a week after the SOP was posted to Web site, WikiLeaks.org claimed that it received an e-mail message from the "Pentagon" (DoD) demanding that the

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Page 14 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

documents posted to the Web site be censored and removed from the Web site. The actual wording of the DoD e-mail message sent to WikiLeaks.org requested that the document be removed from the Web site and that the procedures under the Freedom of Information Act be used to request release of the SOP.^[34]

(U) Leakage of Classified Information to WikiLeaks.org

(S//NF) WikiLeaks.org also posted a report by the National Ground Intelligence Center (NGIC), classified SECRET//NOFORN, entitled “*(U) Complex Environments: Battle of Fallujah I, April 2004,*” (NGIC-1127-7138-06). The NGIC report was the second in a series of reports that analyzed recent warfare in complex environments such as urban environments. See Figure 2. The NGIC report discusses enemy use of asymmetric tactics, techniques, and procedures (TTP) during the Battle of Fallujah in April 2004 and offers many useful lessons learned regarding how a relatively weak adversary can prevent the United States from accomplishing its military objectives. WikiLeaks.org claims the document was leaked by a source it refers to as “Peryton,” who is described as a former employee of NGIC. Both a copy of the actual NGIC classified report (in PDF) and the WikiLeaks.org news article were posted on the WikiLeaks.org Web site. A variety of newspapers, wire services, and other news and media organizations wrote numerous articles based on the original WikiLeaks.org news article and actual classified document posted to their Web site.^[35]

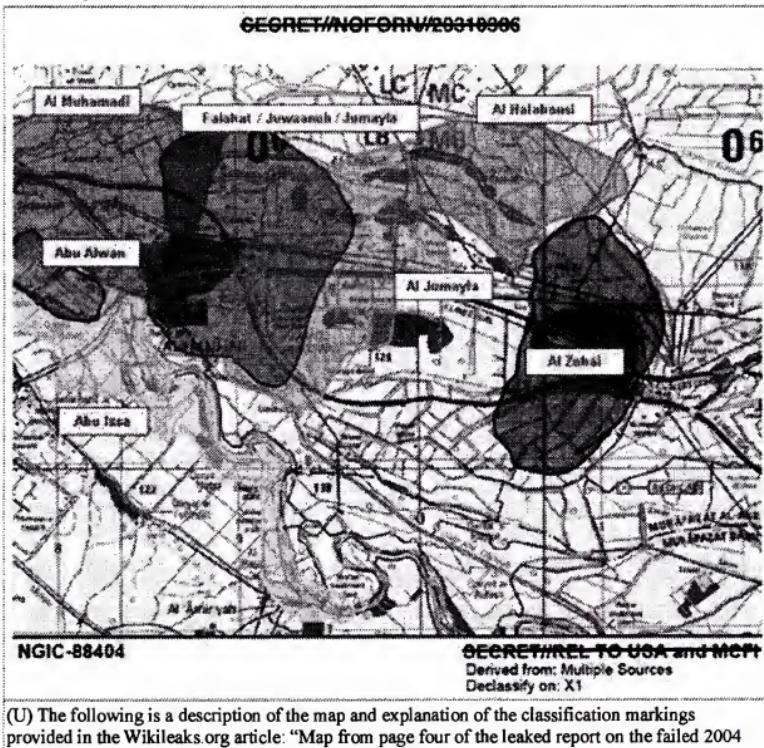
(S//NF) The possibility that a current employee or mole may exist within DoD or elsewhere in the US government who is actively providing sensitive or classified information to WikiLeaks.org cannot be ruled out. Nevertheless, the claim that the leaker is a former NGIC employee is highly suspect, since WikiLeaks.org claims that the protection of the anonymity of the “whistleblower” or “leaker” is one of its primary concerns. In addition, this claim could simply be a crude attempt to mislead investigations into who leaked the document. Use of a code name, incorrect employment information, or incorrect status are most likely rudimentary OPSEC measures designed to protect the identity of the current or former “insider” who leaked the information. In addition, usage of present and past verb tenses and other contradictions in referencing “Peryton” by the WikiLeaks author and staff personnel are most likely part of a deliberate deception, but one cannot completely rule out the possibility that some of these contradictions could be inadvertent OPSEC errors made by authors lacking experience in protecting their methods or sources.

(S//NF) Unclassified e-mail addresses and work telephone numbers of the authors and other persons referenced in the NGIC report were listed in the NGIC document, thus making them available to members of the news media attempting to verify the leaked information. WikiLeaks.org and some other news organizations did attempt to contact the NGIC personnel by e-mail or telephone to verify the information. Such efforts by WikiLeaks.org to verify the information are in contravention to its stated policy not to attempt to verify the information it receives from its sources. WikiLeaks.org went forward with publishing their news article based on the classified NGIC report although they did not receive a response to their inquiry. This is of interest because some journalists exploit the lack of a response to their inquiries by implying that a refusal to respond, failure to respond to a FOIA request, or failure to verify or receive other information presumes that those failing to respond have something to hide. This further weakens

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

the claim that an alleged former NGIC employee leaked the information and strengthens other possibilities. A former NGIC employee would be regarded by many as a highly credible source and either taken at his or her word or asked to provide other bona fides to verify the employment claim. Given the high visibility and publicity associated with publishing this classified report by WikiLeaks.org, however, attempts to verify the information were prudent and show journalist responsibility to the newsworthiness or fair use of the classified document if they are investigated or challenged in court.[36]

SECRET//NOFORN



**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)** Page 16 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

assault on the Iraqi town of Fallujah, which is situated 40 miles from Baghdad. The report is classified SECRET//NOFORN. NOFORN means do not share with US allies such as the UK, Australia, and Canada. 20310603 is date after which 25 years have elapsed and the document would normally be declassified. X1 specifies that the document is exempt from declassification.”

(S//NF) Figure 2. Map from Page 4 of NGIC Report Entitled “(U) Complex Environments: Battle of Fallujah I, April 2004” As Published in a WikiLeaks.org Article.

[\[Back to Table of Contents\]](#)

(S//NF) The author on the WikiLeaks.org staff published the article using selected excerpts and used information that was out of context from the actual NGIC report. The article intertwined classified information from the NGIC report and information gleaned from other news articles in the open media to strengthen its portrayal of the coalition offensive operations in Fallujah in 2004 as a military and political defeat for the United States. The leakage of this NGIC report could allow anti-Coalition forces to portray themselves as victors because they successfully manipulated the media coverage in the April 2004 battle to divide the coalition forces politically and force a halt to the offensive operations. The leaked report could also provide foreign governments, terrorists, and insurgents with insight into successful asymmetric warfare tactics, techniques, and procedures that could be used when engaging US or Coalition forces and provide insight into effective media, information, or influence operations that could be used to defeat a superior enemy.[\[37\]](#)

(U) The catalogue, indexing and filing entry on the WikiLeaks.org Web site for the leaked NGIC document is in *Table 2*, below. This is the information as posted on the WikiLeaks.org Web site.

[\[Back to Table of Contents\]](#)

(S//NF) Table 2. Descriptive Entry of the File and How it is Catalogued by WikiLeaks.org for the NGIC Report Entitled “(U) Complex Environments: Battle of Fallujah I, April 2004” [NGIC-1127-7138-06], as Posted on its Web Site.[\[38\]](#)

File	fallujah.pdf (click to view file)
Analysis	Al Jazeera and Abu Ghraib scuttled US war in Fallujah
Summary	Classified 2006 SECRET//NOFORN report by the US Army National Ground Intelligence Center. “Enemy employment of asymmetric tactics, techniques, and procedures (TTP) during the Battle of Fallujah in April 2004 offers many useful lessons learned in how a relatively weak adversary can prevent the United States from accomplishing its military objectives.”

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Page 17 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

File Size	280144K
File Info	PDF document, version 1.4
File Identity	SHA256 28d7b0d27805749db32f38088c9ecbb963d4564877e723930cf44d8d0c6c7c8e
Wikileaks release	2007-12-24
Country	United States
Organization	US Army National Ground Intelligence Center
Organization type	Military or intelligence (ruling)
Submitted by	Peryton [ACIC comment: this is the code name given by WikiLeaks.org to the leaker(s) of the information.]

SECRET//NOFORN**(U) Technical Skills and Abilities**

(S//NF) WikiLeaks.org developers and technical personnel appear to demonstrate a high level of sophistication in their efforts to provide a secure operating environment for whistleblowers desiring to post information to the Web site. They currently use a variety of indigenously modified free software to build the Web site and route and secure the transmission of data to WikiLeaks.org.

(S//NF) The construction of a SQL database, the merging of leaked documents, and use of publicly available tools to glean information from the Web sites of various DoD and private organizations such as globalsecurity.org and then make the information available in a searchable format, allowing access to and manipulation of the data and information for research purposes by users of WikiLeaks.org, demonstrate a high level of technical capability and resourcefulness.

(S//NF) The current and future intent of the WikiLeaks.org staff and writers is to continue development of enhanced tools for the manipulation of the 2,000 pages of information on US forces by visitors to the Web site. Future efforts may include expanding the use of encryption, operational cyber tradecraft, and physical tradecraft in the delivery and transmission of leaked information for posting to the WikiLeaks.org Web site. It is highly likely that transmission security will improve as new technology, the technical skills of current members, or new funding sources allow. The purchase of more secure equipment, transmission means, and encryption protocols is possible if additional financial resources are made available to the organization.

(U) Is it Free Speech or Illegal Speech?

(U//FOUO) WikiLeaks.org allows anonymous publication of information and records without oversight or accountability; anyone can post information to the Web site, and there is no editorial review, fact checking, or oversight of the posted information. Persons accessing the Web site are encouraged to form their own opinions regarding the accuracy of the information and are

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Page 18 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

allowed to post their own comments. This open policy of posting information and providing commentary could create multiple legal issues for WikiLeaks.org that could subject members to legal prosecution or civil issues by foreign governments, businesses, and individual complainants. In addition, some governments may contend that accessing the Web site itself is a crime, and that shutting down or blocking access to the Web site is a reasonable countermeasure to prevent viewing or downloading of objectionable content. This situation raises the possibility that the WikiLeaks.org Web site could be deliberately used to post fabricated information; to post misinformation, disinformation, or propaganda; or to conduct perception management and influence operations designed to convey a negative message to specific audiences.

(U) Diverse views exist within the United States and other countries regarding the stated goals of WikiLeaks.org. Some believe that the leaking and posting of information is constitutionally protected free speech and supports freedom of the press, open-society initiatives, and government accountability, and that leaking the information serves the greater good versus any illegal acts that arise from the posting of sensitive or classified government or business information. Others believe that WikiLeaks.org or individual persons associated with WikiLeaks.org will face legal challenges in some countries regarding the privacy of individuals and businesses, the revelation of sensitive or classified government information, or the posting of information that is allegedly wrong, false, slanderous, or libelous. Several foreign companies have already filed civil lawsuits in the United States and the United Kingdom for data theft, libel, and damage to their business reputation for the posting of internal and proprietary company information to the WikiLeaks.org Web site. The WikiLeaks.org Web site was temporarily shutdown in late February 2008 for 2 weeks in the United States by court order over the publication of sensitive documents in a case involving a potential money laundering, grand larceny, and tax evasion charges by the Julius Bare Bank in the Cayman Islands and Switzerland. Julius Bare Bank decided to drop the court case against WikiLeaks.org in US courts. The US court order was lifted and the Web site was restored in the United States.

(U) In addition, several prominent bloggers have questioned the usage and reliability of the security of the software used to develop the Web site and to protect communications and identities of leakers. The motives and methods of the WikiLeaks.org developers and members have been questioned, and several bloggers believe that other Internet forums exist that served the same function in a more ethical manner. Efforts by some domestic and foreign personnel to discredit the WikiLeaks.org Web site include allegations that it allows uncorroborated information to be posted, serves as an instrument of propaganda, and is a front organization for the Central Intelligence Agency (CIA). WikiLeaks.org denies these accusations, and no evidence has been presented to support such assertions.[39]

(U//FOUO) Questions and concerns have been raised by media consultants, ethics experts, and other journalists regarding the status of WikiLeaks.org as a news organization and of its staff writers as journalists. The contention by some is that WikiLeaks.org does not qualify as a news organization and thus its staff writers are not journalists. WikiLeaks.org's desire to expose alleged wrongdoing by revealing sensitive or classified government or business information, in effect, encourages the theft of sensitive or classified proprietary information or intellectual property. In doing so, some argue, WikiLeaks.org is knowingly encouraging criminal activities such as the theft of data, documents, proprietary information, and intellectual property, possible violation of

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

national security laws regarding sedition and espionage, and possible violation of civil laws. Within the United States and foreign countries the alleged "whistleblowers" are, in effect, wittingly violating laws and conditions of employment and thus may not qualify as "whistleblowers" protected from disciplinary action or retaliation for reporting wrongdoing in countries that have such laws. Also, the encouragement and receipt of stolen information or data is not considered to be an ethical journalistic practice. In addition, the sources of WikiLeaks.org staff writers are not verified, nor are its news articles fact-checked or confirmed by additional sources, as customary in news organizations. Moreover, there is no editorial review of the articles prior to publication. Finally, some critics contend that the staff writers are biased and have made unsupportable claims to support political agendas to effect change in government or business policy. [40]

(U) Several countries have complained publicly or blocked access to WikiLeaks.org and similar Web sites and have asserted claims that they have the right to investigate and prosecute WikiLeaks.org members and whistleblowers. In addition, several countries also claim the right to remove false information, sensitive or classified government information, propaganda, or other malicious content from the Internet. As a result, WikiLeaks.org members have already posted information in China on how to circumvent blocks to the Web site imposed by the Chinese government for having objectionable content related to the participation of Chinese dissents in WikiLeaks.org and to pro-democracy issues. [41]

[\[Back to Table of Contents\]](#)

(U) Intelligence Gaps

- (S//NF) What individual persons or entities are leaking DoD sensitive or classified information to WikiLeaks.org, and are they working on behalf of a foreign agent or power? What are the reasons, intentions, and motivations of the current or former insider?
- (S//NF) Is the potential insider leaking the information to WikiLeaks.org a former employee of the US government or a mole still working for the US government? How is the insider sending digital information to WikiLeaks.org? What cyber or other tradecraft is the perpetrator using?
- (S//NF) Will the WikiLeaks.org Web site be used by FISS, foreign military services, foreign insurgents, or terrorist groups to collect sensitive or classified US Army information posted to the WikiLeaks.org Web site?
- (S//NF) Will the WikiLeaks.org Web site be used by FISS, foreign military services, or foreign terrorist groups to spread propaganda, misinformation, or disinformation or to conduct perception or influence operations to discredit the US Army?
- (S//NF) Will the WikiLeaks.org Web site be used for operational or cyber tradecraft to pass information to or from foreign entities?
- (S//NF) Will the WikiLeaks.org Web site developers obtain new software for Web site development, management, security, encryption of messages or files, or posting anonymous information to the Web site?
- (S//NF) From what foreign personnel or groups does WikiLeaks.org receive funding or collaborate with for sharing information or development of new software?

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Page 20 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

- (S//NF) Will foreign entities attempt to conduct CNE or CNA to obtain information on the posters of information or block content on the WikiLeaks.org Web site?
- (S//NF) What software, tactics, techniques, and procedures would be used by a foreign actor to conduct CNE or CNA against the Web site?
- (S//NF) Will foreign persons, businesses, or countries attempt civil lawsuits or criminally prosecute whistleblowers, WikiLeaks.org staff, and members who posted comments on the Web site?
- (S//NF) Will WikiLeaks.org and various users expand the data fields in the TOE SQL database to include equipment capabilities, equipment limitations and vulnerabilities, known unit locations, links to geospatial information services, or known unit personnel to develop "battle books" for targeting packages?
- (S//NF) What other leaked DoD sensitive or classified information has been obtained by WikiLeaks.org?
- (S//NF) Will foreign organizations such as FISS, foreign military services, foreign insurgents, or terrorist groups provide funding or material support to WikiLeaks.org?

[\[Back to Table of Contents\]](#)

(U) Conclusions

(S//NF) Web sites such as WikiLeaks.org have trust as their most important center of gravity by protecting the anonymity and identity of the insider, leaker, or whistleblower. Successful identification, prosecution, termination of employment, and exposure of persons leaking the information by the governments and businesses affected by information posted to WikiLeaks.org would damage and potentially destroy this center of gravity and deter others from taking similar actions.

(U//FOUO) The unauthorized release of DoD information to WikiLeaks.org highlights the need for strong counterintelligence, antiterrorism, force protection, information assurance, INFOSEC, and OPSEC programs to train Army personnel on the proper procedures for protecting sensitive or classified information, to understand the insider threat, and to report suspicious activities. In addition, personnel need to know proper procedures for reporting the loss, theft, or comprise of hard or soft copy documents with sensitive information or classified information to the appropriate unit, law enforcement, or counterintelligence personnel. Unfortunately, such programs will not deter insiders from following what they believe is their obligation to expose alleged wrongdoing within DoD through inappropriate venues. Persons engaged in such activity already know how to properly handle and secure sensitive or classified information from these various security and education programs and has chosen to flout them.

(S//NF) It must be presumed that WikiLeaks.org has or will receive sensitive or classified DoD documents in the future. This information will be published and analyzed over time by a variety of personnel and organizations with the goal of influencing US policy. In addition, it must also be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the WikiLeaks.org Web site. Web sites similar to WikiLeaks.org will continue to proliferate and will continue to represent a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army for the foreseeable future.

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Sensitive or classified information posted to WikiLeaks.org could potentially reveal the capabilities and vulnerabilities of US forces, whether stationed in CONUS or deployed overseas.

(S//NF) The proliferation of access to Internet, computer, and information technology technical skills, software, tools, and databases will allow the rapid development, merging, integration, and manipulation of diverse documents, spreadsheets, multiple databases, and other publicly available or leaked information. Possible enhancements could increase the risk to US forces and could potentially provide potential attackers with sufficient information to plan conventional or terrorist attacks in locations such as Iraq or Afghanistan.

(S//NF) The various open or freeware applications used in the development and management of WikiLeaks.org continue to improve with time. Several Internet software development companies, foundations, electronic privacy organizations, database management services, encryption developers, and anonymous e-mail services can generate sufficient income, accept donations, and use volunteers to continue to develop and improve the software. Improvements in these software applications will provide greater privacy and anonymity of persons who leak information to WikiLeaks.org.

(S//NF) The possibility that various computer experts, researchers, and users could expand the data fields in the TOE SQL database to include pictures; equipment capabilities, limitations and vulnerabilities; known unit locations; links to geospatial information; and known unit personnel cannot be ruled out. The continued development of new technologies for merging and integrating various geographic or other information services into easy-to-use databases could allow rapid compilation of unit profiles that could be used for developing actionable information for use by FISS, foreign terrorist organizations, and other potential adversaries for intelligence collection, planning, or targeting purposes [42]

[\[Back to Table of Contents\]](#)

(U) Point of Contact

(U) This special report was produced by the Army Counterintelligence Center (ACIC). ACIC POC is Michael D. Horvath, Senior Analyst, Cyber CI Assessments Branch, commercial, 301-677-2489 or DSN 622-2489.

[\[Back to Table of Contents\]](#)

(U) Appendix A: Glossary

(U) **FreeNet (or Freenet).** Freenet is a decentralized and censorship-resistant distributed data storage system. Freenet aims to provide freedom of speech through a peer-to-peer network with strong protection of anonymity. Freenet pools contributed bandwidth and storage space of member computers in the network to allow users to anonymously publish or retrieve various

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

Page 22 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

kinds of data or information. The storage space is distributed among all connected nodes on Freenet.[\[43\]](#)

(U) Google Earth. Google Earth is a geographic information system (GIS) using the Google search engine that permits interactive viewing of digital satellite imagery, maps, terrain, and 3D buildings.[\[44\]](#)

(U) MediaWiki. Wikipedia runs on its own in-house-created software, known as MediaWiki, a powerful, open-source wiki system written in PHP and built upon MySQL. As well as allowing articles to be written, it includes a basic internal macro language, variables, transcluded templating system for page enhancement, and features such as redirection.[\[45\]](#)

(U) OpenSSL. The OpenSSL Project is a collaborative effort to develop an easy-to-use Open Source toolkit implementing the Secure Sockets Layer and Transport Layer Security protocols with encryption. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation. The OpenSSL toolkit is licensed in a manner that allows free usage for commercial and noncommercial purposes subject to some simple license conditions.[\[46\]](#)

(U) PGP. PGP (Pretty Good Privacy) is an application and protocol for secure e-mail and file encryption developed by Phil Zimmerman. PGP was originally published as freeware, and the source code has always been available for public use and adaptation. PGP uses a variety of algorithms, such as IDEA, RSA, DSA, MD5, and SHA-1 for providing encryption, authentication, message integrity, and private and public-key management. PGP is based on the "Web-of-Trust" model and is the most popular encryption system used by individual personnel, businesses, and governmental entities throughout the world to protect or hide content on the Internet.[\[47\]](#)

(U) SQL. SQL (Structured Query Language) is also known as Database Language SQL (S-Q-L), is a computer language designed for the retrieval and management of data in a relational database management system, database schema creation and modification, and database object access control management. SQL is a standard interactive and programming language for getting information from and to update a database. Queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth.[\[48\]](#)

(U) SQLite. SQLite is a public domain software library that implements a self-contained, serverless, zero-configuration application that does not require setup or administration, cross platform, transactional SQL database engine that can support terabyte-sized databases and gigabyte-sized strings and blobs. SQLite is the most widely deployed SQL database engine in the world. The software application is used in countless desktop computer applications as well as consumer electronic devices including cellular phones, Personal Digital Assistants, and MP3 players. The source code for SQLite is in the public domain. SQLite is a popular choice as the database to back small-to-medium-sized Web sites because it requires no or little configuration and stores information in ordered disk files that are easy to access and will preserve transactions after system crashes or power outages. SQLite is a completely self contained application that has

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

a small code print (250KB size fully configured) and is a faster client/server for common operations. [49]

(U) **TOR (or Tor).** Tor (The Onion Router) is a network of virtual tunnels that allows people or various groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." [50]

(U) **Traffic analysis.** Traffic analysis is a form of pattern and usage analysis that can be used to infer who sending or receiving e-mail and data exchanges on a private network, public network, or the Internet. Knowing the source and destination of Internet traffic allows individuals, criminals, law enforcement, and intelligence and security services to track the activities, behavior, and interests of the sender or receiver. This form of pattern analysis can be used to identify persons and possibly threaten a person's employment and physical safety by revealing who and where they are located. [51]

(U) **Web servers.** Web servers are computer hardware that stores HTML documents, images, text files, scripts, and other Web-related data, collectively known as content, and distributes this content to other clients on the network upon request.

(U) **Wiki.** A wiki is a type of Web site that allows users to easily add, remove, or otherwise edit and change some available content, sometimes without the need for registration. This ease of interaction and operation makes a wiki an effective tool for collaborative authoring. The term wiki can also refer to the collaborative software itself (wiki engine) that facilitates the operation of such a Web site or to certain specific wiki sites and the online encyclopedias such as Wikipedia. Wiki was created in 1994 and installed on the Web in 1995 by Ward Cunningham. [52]

(U) **Wikipedia.** Wikipedia is a blend of the words *wiki* and *encyclopedia*. Wikipedia is a multilingual, Web-based free content encyclopedia project operated by the nonprofit Wikimedia Foundation. Wikipedia is written collaboratively by volunteers, allowing most articles to be changed by almost anyone with access to the Web site. Wikipedia's main Web servers are in Tampa, FL, with additional Web servers in Amsterdam and Seoul. [53]

[\[Back to Table of Contents\]](#)

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

(U) Appendix B: Methodology Used by Authors for Analysis of Leaked Tables of Equipment for US Forces in Iraq and Afghanistan

(U) A WikiLeaks.org staff writer, Julian Assange, with assistance from several other persons developed a SQL data base to store the 2,000 pages of leaked TOE information and merged information from other sources into a usable data base for research purposes. The entire SQL database developed by the authors for the TOEs was posted on the WikiLeaks Web site for anyone to use. The following is a list of steps purportedly used to make the data easy to use and accessible for persons wanting to conduct their research.

1. Julian Assange and other persons that assisted him used publicly available open-source information to learn and understand the abbreviations, acronyms, numbers, and other nomenclatures in the leaked information, specifically NSN (NATO Stock Number), LIN (Line Item Number), and UIC (Unit Identification Code). The authors compiled their results and documented the information on US military logistics in a separate document on the Web site.
2. They then found various public NSN catalogues on the Internet, which were used to confirm the validity of random samples of the leaked information using these databases and other deployment references.
3. By hand, they created tallies for a select list of interesting items through their observations of the reviewed information within the database. They wrote a draft report based on their research and analysis of the database and other publicly available information.
4. They then used software and software applications such as VIM macros, PERL scripts, and several Python programs to organize the material into a more presentable spreadsheet format (such as Afghanistan OEF Property List and Afghanistan OEF Property List.html).
5. They wrote additional software code to merge data from several NATO Logistics spreadsheets, which allowed the NSNs to be organized into subcategories to identify the NATO Supply Group and NATO Supply Classification for the equipment.
6. They obtained a list of NATO Supply Group and NATO Supply Classification codes from public US military logistics sources available on the Internet that was merged with other spreadsheets.
7. They used SQL to install a database program.
8. They merged the original leaked data into group and classification code tables using a SQL database, in this case using SQLite. The authors noted that any SQL database could have been used to index and catalogue the information.
9. They used SQL to merge NATO Supply Classifications with leaked data to provide extra context and generate Afghanistan OEF Property List-extended.html.

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)** Page 25 of 32

**SECRET//NOFORN
(UNCLASSIFIED//FOUO UPON REMOVAL OF REFERENCES)**

10. Using SQL, they generated several different indexes and tallies for the leaked items, by NATO Supply Group, NATO Supply Classification, and NSN. This data was then converted into HTML format and placed into an appendix.
11. Again using SQL, they generated a unique list of NSNs. They wrote a script or software program to concurrently query the US logistics Web-query NSN search for pricing information and extract the price for every NSN on the list (except for alphanumeric NSNs, which are not listed, probably due to being Management Control Numbers).[54]
12. They merged pricing information into the SQL database.
13. They used SQL to generate a new tally by NSN, merged this with the pricing information for each NSN, sorted by the total price, converted the data to HTML, and placed it into the Appendix.
14. They used SQL to calculate the total value of all equipment for which they had cost information.
15. They examined the data and extracted additional information that was of interest such as notable units and items of equipment.[55]

Prosecution Exhibit 46

32 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

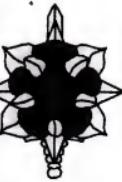
stored in the classified

supplement to the original

Record of Trial

Prosecution Exhibit 47
has been entered into
the record as a CD/DVD
and will be maintained
with the original
Record of Trial

Prosecution Exhibit 48
has been entered into
the record as a CD/DVD
and will be maintained
with the original
Record of Trial



Issue: Islamic Extremism



- Martyrdom - Life on earth is for suffering
- No secular government
- Conversion or destruction - Zero tolerance for other religions (or any version of Islam differing from their own)
- Convert entire world to their vision of Islam

*Think about the entire world looking like
Afghanistan under the Taliban*



The Impact of Islamic “End of Time” Expectations



- The Elimination of God's Enemies
- The World Subdued
- The Coming of the “Mahdi”



**Muhammad Ahmad
ibn as Sayyid Abd
Allah (1884)**



**Hazrat Mirza Ghulam
Ahmad Qadiani
(1835-1908)**



Usama bin Ladin



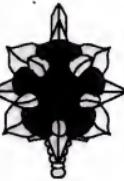
Terrorism



US Department of State

Title 22 of the US Code, Section 2656f(d)

- **Terrorism:**
Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience
- **International Terrorism:**
Terrorism involving citizens or the territory of more than one country
- **Terrorist Group:**
Any group practicing, or that has significant subgroups that practice, international terrorism



The Impact of Islamic Extremism on Regional / Global Relations

Islamist's Perception

● of Their Enemies

- Islam vs. The State of Israel
- Islam vs. The West
- Islam vs. The Modern World



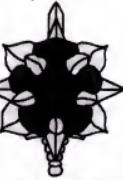


Al Qaeda

AKA: Usama Bin Ladin Organization



- **Extreme Sunni (Wahabi) Islam**
- **NO religious tolerance**
- **Loose structure, little secrecy about leadership**
- **Network with many other like-minded groups**
- **State support (?)**



Ansar al-Islam (AI)

AKA: Helpers of Islam, Kurdish Taliban



Mullah Krekar

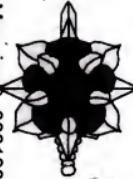
- Kurdish Islamist group
- Established In 2001
- At odds with other Kurdish groups
- Linked to al-Qaeda & Zarqawi
- Responsible for 30 suicide bombings in Iraq



Ansar al-Sunnah (AS)

- Dedicated to the establishment of an Islamic state
- Members vary; Ansar al-Islam, foreign al-Qaeda operatives and Iraqi Sunnis
- Sees Kurdish political establishment as a puppet regime of the American occupation





Abu Ayyub al-Masri, an Egyptian operative is believed to be the new leader of Al Qaeda in Iraq.

Tanzim Qaeda al-Jihad fi Bilad al-Rafidayn (QJBR)
AKA: Al Qaeda in Iraq (AQI), Tawhid and Jihad, AQIZ



- “**Monotheism and Holy War**”
 - The al Qaeda Group for Jihad in Iraq
- **Ties to al-Qaeda**
- **Kidnappings and executions**
- **Has also attacked Iraqi Police & Security Forces**



Issue: Extremist Recruiting



Baghdad, Occupied Iraq, March 20, 2004



Using the Iraq War as their main Terrorist Recruitment Tool



Recruiting

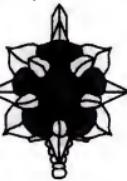


Baghdad
April 2003



**Islamic extremists are exploiting the
Iraqi conflict to recruit new anti US
Jihadists.**

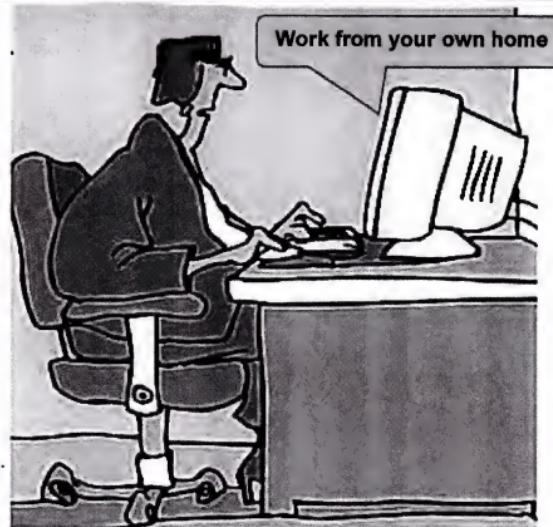
Recruiting



Women are now being recruited



Recruiting



"No thanks, just browsing."

Over the last ten years, the number of terrorist sites has jumped from less than 100 to as many as 4,000. Many insurgency groups have many sites and message boards to help their network.²²³



Mission End State

- **Various and Complex**
- – Nothing to Lose
- Religious Duty
- Only Guarantee of Paradise



The Brutal Present



The Idyllic Future



Mission End State

Al Qaeda, QJBR, Ansar al-Sunnah & Ansar al-Islam

To unite Muslims to fight the United States as a means of defeating Israel, overthrowing regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries. The establishment of a pan-Islamic caliphate throughout the world.





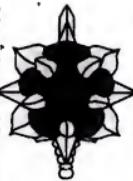
Mission End State

“Eventually all people must become Muslim, including the Christians and Jews of the United States. The world has to go the way we want. It's our divine right to lead humanity.”

- Mohammed Ajmal Qadri

Leader of the fundamentalist
Jamiat Ulema Islam Party





Student Check



**Name the four Terrorist Groups
covered in the lesson.**

Al Qaeda

Ansar al-Islam

Ansar al-Sunnah

Al Qaeda in Iraq

QUESTIONS?



305th MI Battalion



Information Security AR 380-5

PROSECUTION EXHIBIT 52 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE OF PAGES

y2



Terminal Learning Objective



ACTION: Identify principles of protecting classified information, material and media.



CONDITIONS: Given simulated classified documents or electronic media and AR 380-5.



STANDARDS: Identify principles of protecting classified Information, Material and Media IAW AR 380-5 by achieving 80% on a culminating examination.



Administrative Data



SAFETY REQUIREMENTS: NONE

RISK ASSESSMENT LEVEL: LOW

ENVIRONMENTAL CONSIDERATIONS: NONE

EVALUATION: Student will be evaluated by use of Practical Exercises, Student Checks, Homework and pass Information Security Exam with 80% accuracy.



Agenda



ELO A: Annotate Classification Markings to a Document

ELO B: Apply Procedures for Protecting Classified Information

ELO C: Provide Information about Operation Security and the World Wide Web



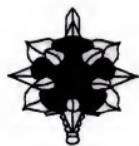
Enabling Learning Objective A



ACTION: Annotate the Proper Classification Markings to Documents and/or Media.

CONDITIONS: Given AR 380-5, classroom instruction and simulated classified document/media.

STANDARD: Annotate simulated classified documents and/or media by achieving 12 of 15 answers correctly on given performance objective IAW AR 380-5.

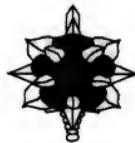


ELO Agenda



ELO A: Annotate Classification Markings to Documents/Media

- **Classification Process**
- **Classification Criteria**
- **Document Markings**
- **Declassification Programs**



Classification Designations



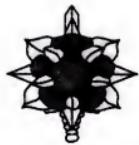
AR 380-5, page 10, para 2-10

Confidential - Cause Damage

Secret - Cause Serious Damage

Top Secret - Cause Exceptionally Grave Damage

To National Security.



Classification Process

page 9, para 2-7



In making a decision to originally classify an item of information, an original classification authority will:

- a. Determine that the information has not already been classified
- b. Determine that the information is eligible for classification
- c. Determine that classification of the information is a realistic course of action and that information can be protected from unauthorized disclosure when classified.
- d. Decide that unauthorized disclosure could reasonably be expected to cause damage to national security.



Classification Process (continued)



page 9, para 2-7

- e. Select the appropriate level or category of classification and/or sensitivity to be applied to the information, based on a judgment as to the degree of damage unauthorized disclosure could cause
- f. Determine and include appropriate declassification, downgrading, and/or exemption instructions to be applied to the information.
- g. Make sure that the classification decision is properly communicated so that the information will receive appropriate protection.



Classification Criteria

page 9, para 2-8



- Military Plans, Weapons Systems, or Operations
- Foreign Government Information
- Intelligence Activities, sources or methods
- Foreign Relations Or Activities Of The US
- Scientific, Technological, Or Economic Matters Relating To National Security
- US Government Programs For Safeguarding Nuclear Materials Or Facilities
- Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security



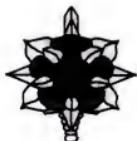
Prohibitions and Limitations

page 9-11, para 2-8, 2-15



- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a Person, Agency or Organization
- Restrain competition

US classification can only be applied to information that is owned by, produced by or for, or is under the control of the US government.



Document Marking

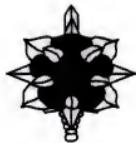
page 23, para 4-4 thru 4-10



Markings will include:

- **Highest level of classification of information contained in the document.**
- **Caveats, when necessary**
- **Classified By:**
- **Reason:**
- **Declassification On:**
- **Date of Source:**

Be sure to include the information that goes with these 4 items



Document Marking

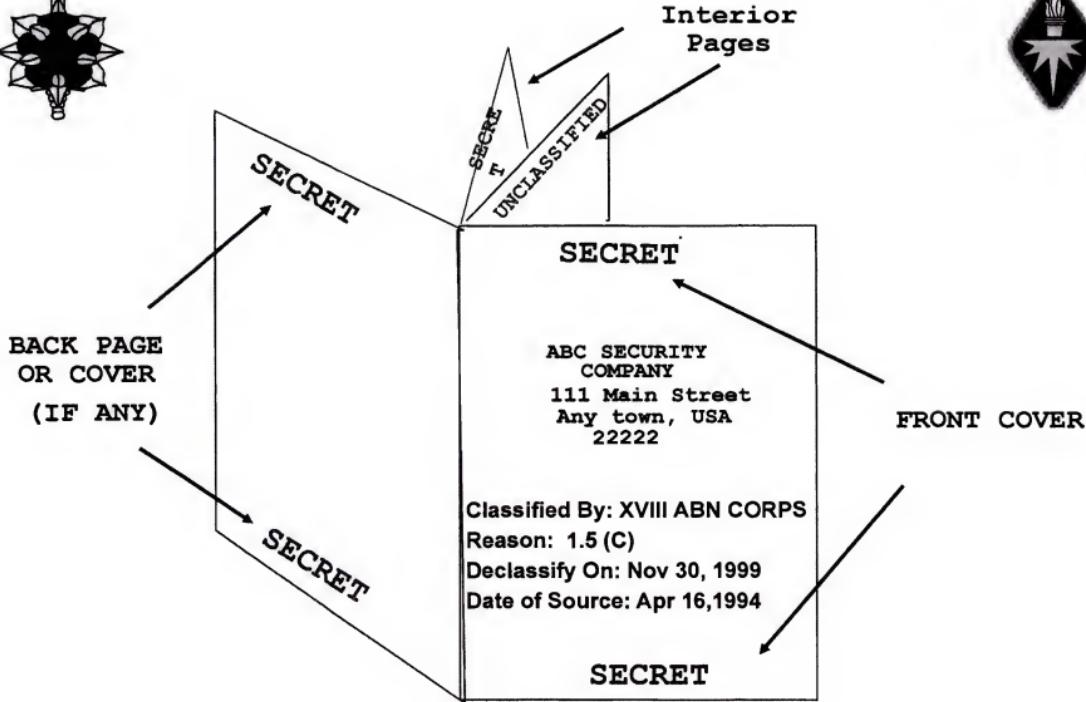
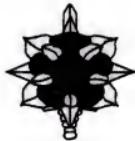
page 22, para 4-4



ALL pages will be marked (centered, top and bottom) with highest classification of information on each page (no abbreviations and capitalized).

To include the title page, front page and the front and back of cover pages.

**TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED**





Document Marking

page 22, para 4-6



At the beginning of paragraphs and sections will be markings with the appropriate abbreviated classification in parenthesis such as:

(TS) for **TOP SECRET**

(S) for **SECRET**

(C) for **CONFIDENTIAL**

(U) for **UNCLASSIFIED**



DOCUMENT MARKING/CAVEATS

page 23, para 4-6



Examples of Paragraph and Portion Markings:

- **(S/NOFORN) – Secret, No Foreign Nationals**
- **(TS/REL NATO) – Top Secret, Releasable to
NATO**
- **(TS/REL GBR) – Top Secret, Releasable to
Great Britain**

Notice the single slash between the Classification and the caveat



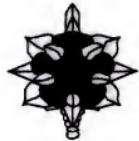
Unclassified Document Marking



Unclassified material that is used for training will be clearly marked showing they are UNCLASSIFIED.

An appropriate statement will be placed on the top and bottom of each page.

- “**UNCLASSIFIED**”
- “**FOR TRAINING PURPOSES ONLY**”- FTPO
- “**FOR OFFICIAL USE ONLY**”- FOUO



Unknown Document Marking



**Material that is produced by an individual,
suspected to be classified but not offered
any guidance must be marked with:**

**“Classification Determination Pending.
Protect at Appropriate Classification
Level.”**



S
T
U
D
E
N
T

C
H
E
C
K

Subject: Sample of Unclassified subject line

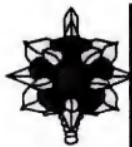
1. [REDACTED] For training purposes this paragraph contains Secret information. It must be marked accordingly.
2. [REDACTED] For training purposes this paragraph contains Confidential information and is for US personnel only. Reason: 1.5(a), mark accordingly.

[REDACTED] 101st ABN DIV

Reason: 1.5(a)

Declassify on: 26 March 2024

Date of Source: 26 March 1999



TOP SECRET

Subject: Sample of Unclassified subject line (U)

- 1.(TS)** For training purposes this paragraph contains Top Secret information. It must be marked accordingly.

- 2. (C)** For training purposes this paragraph contains Confidential information. It must be marked accordingly.

Classified by: G2, 101st ABN DIV

Reason: 1.5(a)

Declassify on: 26 March 2024

Date of Source: 26 March 1999

TOP SECRET



Declassification Programs

page 14, para 3-1



Department of the Army files and records will not be declassified without prior review to determine if continued classification is warranted and authorized.

- (1) Original classification authority action**
- (2) Automatic (Per Executive order)**
- (3) Mandatory**
- (4) Systematic**



Student Checks



What are 3 unclassified document markings?

**UNCLASSIFIED
FOUO
FTPO**

What are the 3 classification levels?

**Top Secret
Secret
Confidential**



QUESTIONS???





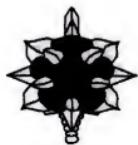
Enabling Learning Objective B



ACTION: Apply Procedures for Protecting Classified Information.

CONDITIONS: Given AR 380-5, classroom instruction and simulated classified information and or media.

STANDARD: Applied security regulations and procedures for protecting classified documents and/or media by achieving 12 of 15 answers correctly on given performance objective IAW AR 380-5.



ELO Agenda



ELO B: Apply Procedures for Protecting Classified Information

- General Restrictions for Access**
- Accountability and Administrative Procedures**
- Storage and Safekeeping of Classified Material**
- Identify Methods of Destruction**



General Restrictions on Access

page 63, para 6-1



Access Will Be Granted Only When:

- **Verification of Security Clearance – Joint Personnel Adjudication System (JPAS)**
- **The Person Has A Need-to-know The Information**
- **The Person Has Signed A Nondisclosure Agreement (SF 312)**



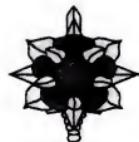
Sensitive Compartmented Information



Classified information concerning or derived from intelligence sources, methods or analytical process, which is required to be handled within formal control systems.

The three SCI control systems are:

- HUMINT, COMINT and TALENT KEYHOLE.**



SCI Control Systems



- **HUMINT**- protects sensitive clandestine HUMINT sources, methods and reporting.
- **COMINT** – protects Electronic Emanations systems and products, a form of Signal Intelligence
 - **GAMMA** – a sub-control Control system
- **TALENT KEYHOLE**- protects satellite recon systems and products/Imagery Intelligence



Determining Responsibility

page 1, para 1-5



Headquarters, Department of the Army (HQDA)-

The Deputy Chief of Staff for Intelligence (DCSINT) is designated as the DA senior official of the Intelligence Community.

- Direct, administer, and oversee the Army information security program.
- Responsible for Information Security matters for units that no longer exist and have no successors.



Determining Responsibility

page 2, para 1-6, 1-7

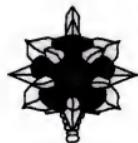


The Commander

- Commanders, Officers in Charge, and head of agencies and activities will effectively manage information security programs within their command.
- Commanders may delegate the authority to execute the requirements of AR 380-5, but not the responsibility to do so.

The Command Security Manager-

is the principal advisor to the commander on Information Security.



Individual Responsibility

page 3, para 1-9



- All personnel have an official responsibility to safeguard classified information.
- All personnel will report any violations or anything that could lead to the unauthorized disclosure of classified and sensitive information.



Violations

page 105, para 10-2



- Anyone **FINDING** classified material out of proper control, will take custody of and safeguard the material and immediately notify the Command Security Manager.
- Anyone becoming aware of possible **LOSS** or **COMPROMISE** of classified information will immediately report it to the Command Security Manager.
- Anyone **IDENTIFYING** classified information in the public media, do not make a comment or statement that will confirm or deny the information and immediately notify the Command Security Manager.



Student Check



What are the 3 SCI control Systems?

**HUMINT
COMINT
TALENT KEYHOLE**



Accountability and Admin Procedures



page 73, para 6-21

Top Secret Information:

- Provided continuous control and accountability.
- Top Secret Control Officers will be designated within offices that hold TS material.
- TS material will be accounted for by receipts; held five years.
- TS material will be inventoried at least once annually by two properly cleared personnel.



Accountability and Admin Procedures



page 74, para 6-22

Secret and Confidential Information:

- Commands will establish procedures to control all Secret and Confidential information IAW AR 380-5.
- Material originated, received, distributed, or routed to sub-elements, and information disposed of will be controlled and accounted for.



Accountability and Admin Procedures



page 74, para 6-24

Working Papers are documents/materials accumulated or created in preparation of finished documents/materials.

- **Papers that contain classified information will be:**
 - Dated when created.
 - Marked as “Draft” or “Working Papers” on the first page.
 - Marked with the highest classification of information within the papers.
 - Protected in accordance with assigned classification.
 - Destroyed when no longer needed.
 - Accounted for, controlled, and marked.
- **180 Day Rule (Review to determine if still needed)**



Storage and Safekeeping





Storage Standards

page 78, para 7-3



Classified information must be secured under adequate conditions to limit access by unauthorized personnel.

- General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for:
 - Containers
 - Vault Doors
 - Alarm Systems
 - Associated security devices suitable for storage and protection of classified material.



Storage and Safekeeping

page 78, para 7-4



Top Secret Material:

- Continuous protection by cleared personnel
- **GSA** approved security container with one of the following supplemental controls:

– Cleared/duty personnel will inspect the container once every two hours (no pattern)

– Intrusion Detection Systems

Secret/Confidential Material:

- GSA approved security container without supplemental controls.



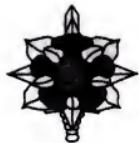
Control Measures

page 67, para 6-9



Commands will maintain measures that ensure access to classified information is limited only to authorized personnel including:

- **Technical (Cameras, Passwords)**
- **Physical (Doors, Guards, Safes)**
- **Administrative (Security Checks)**
- **Personal (Investigations)**
- **Personnel Control (Access Rosters)**

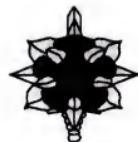


Control Measures

page 67, para 6-9, 6-10



- DA personnel are responsible for ensuring that unauthorized persons do not gain access to classified information.
- Classified information will be protected at all times either by storage, having it under personal observation and physical control of an authorized individual.



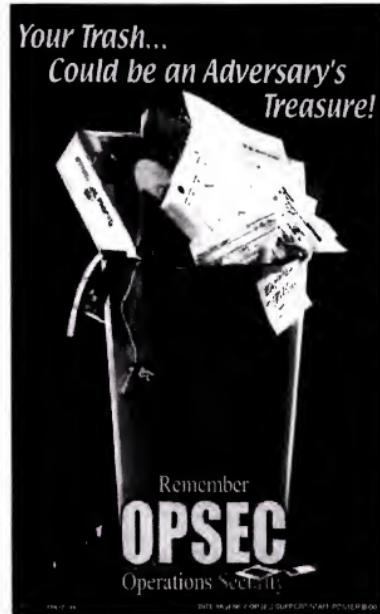
Control Measures

page 67, para 6-11



- At the end of the work day a system of security checks will be done to ensure classified material is properly secured.

- The SF 701 (Activity Security Checklist) will be used to record end-of-day security checks.





Control Measures

page 67, para 6-10



Classified document cover sheets will be placed on classified documents or files not in security storage.

- SF 703 (**TOP SECRET** Cover Sheet)
- SF 704 (**SECRET** Cover Sheet)
- SF 705 (**CONFIDENTIAL** Cover Sheet)



CONFIDENTIAL INFORMATION

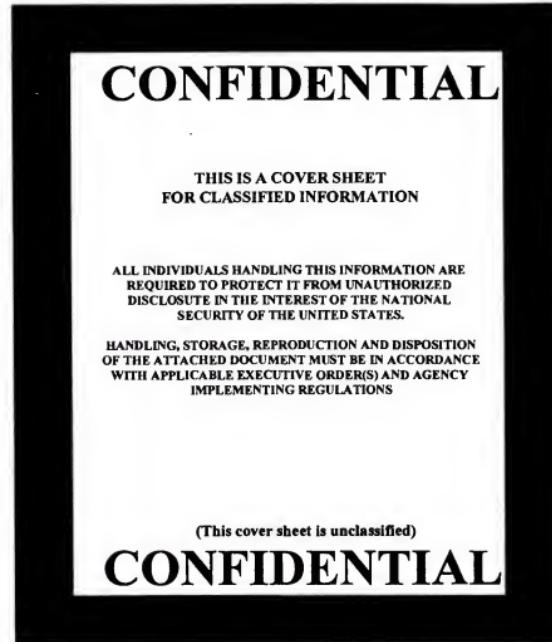


SF 705

**LOWEST LEVEL OF
CLASSIFIED
INFORMATON**

Paragraph 2-10, AR 380-5

CONFIDENTIAL:
Information or material
that when disclosed
could be expected to
cause damage to U.S.
security.





SECRET INFORMATION



SF 704

**MIDDLE LEVEL OF
CLASSIFIED
INFORMATON**

Paragraph 2-10, AR 380-5

**SECRET:
Information or material
that when disclosed could
be expected to cause
serious damage to U.S.
security.**





TOP SECRET INFORMATION



SF 703

**THE
HIGHEST LEVEL OF
CLASSIFIED
INFORMATION**

Paragraph 2-10, AR 380-5

TOP SECRET
Information or material
that when disclosed could
be expected to cause
exceptionally grave
damage to U.S. security.

TOP SECRET

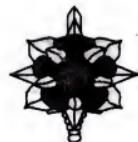
THIS IS A COVER SHEET
FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE
REQUIRED TO PROTECT IT FROM UNAUTHORIZED
DISCLOSURE IN THE INTEREST OF THE NATIONAL
SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION
OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE
WITH APPLICABLE EXECUTIVE ORDER(S) AND AGENCY
IMPLEMENTING REGULATIONS

(This cover sheet is unclassified)

TOP SECRET



Labeling Computers & Media

page 31, Section III



- **Laptop Computers**
- **Desktop Computers**
- **Printers**
- **Scanners**
- **Copiers**
- **Fax Machines**
- **Disks, Flash Drives, CD's, etc...in a
classified environment**





Control Measures

page 33, para 4-34



Classified labels will be placed on all classified Automated Data Processing media



SF 708



SF 707

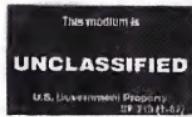
Others that may be used/seen:

**SF 711 - Data Descriptor Label
(yellow & black)**



SF 706

**SF 712 - CLASSIFIED SCI Label
(yellow & white)**



SF 710



Nicknames as a Control Measure



Appendix H, page 212

Nickname – A combination of two separate unclassified words which is assigned an unclassified meaning and is employed only for unclassified administrative, morale or public information purposes.

Operation Iraqi Freedom

Not a correct example of a Nickname!



Student Checks



**What are the five control measures to
Limit access to classified material?**

Technical ↔ Cameras, Passwords

Physical ↔ Doors, Guards, Safes

Administrative ↔ Security Checks

Personal ↔ Investigations

Personnel ↔ Access Rosters

What are some examples?



QUESTIONS???





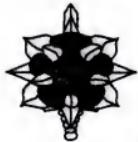
Transmission/Transportation of Classified Documents



page 90, para 8-2

Top Secret

- Authorized Cryptographic system
- Defense Courier Service
- Authorized or Command courier/messenger service
- Department of State Diplomatic Courier Service
- Cleared U.S. Military personnel, U.S. Government civilian and DOD contractor employees



Transmission/Transportation of Classified Documents



page 90, para 8-3

Secret

- Any means approved for TOP SECRET
- U.S. Postal Service registered Mail and Express Mail within the 50 states, DC and Puerto Rico
- U.S. Postal Service Registered Mail through Military facilities (APO/FPO) when outside of the U.S and its territories. As long as it does not pass through foreign postal system or any foreign inspection

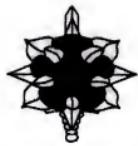


Prepare to Mail Classified Documents

page 94, para 8-9/10



- Brown Opaque envelopes
- Packing Tape
- Classification Stamp/Red Pen
- Registered Mail Certificate
- Classified Document receipt (DA Form 3964)
- Classified Document (**SECRET & CONFIDENTIAL only**)
- Inspect the document to ensure that all markings are present and correctly placed on both sides



STEP ONE



CLASSIFICATION FOR TRAINING PURPOSES ONLY
SECRET/NOFORN



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
FOR COMMAND, CONTROL, COMMUNICATIONS, AND
INTELLIGENCE

May 25, 2004

- Document Folded into Thirds



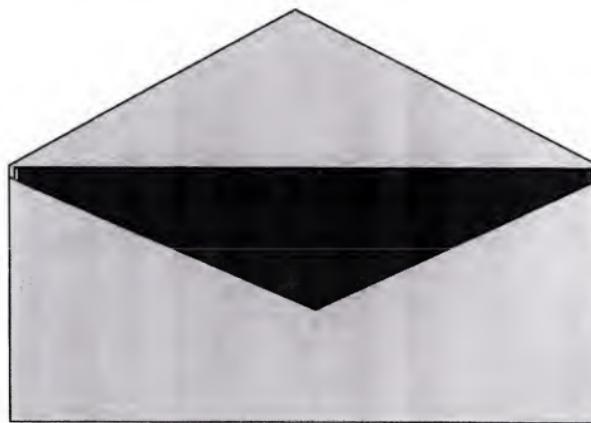
STEP TWO



- **Final Folded Document**



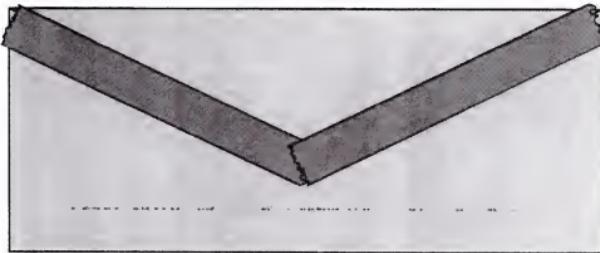
STEP THREE



- Into an Opaque Envelope



STEP FOUR



- **Tape Seams**



STEP FIVE



- Tape Outer Seams



STEP SIX



- **Address and Classification Markings**

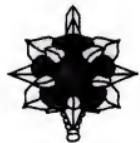


Address/Classification Markings for Inner envelope

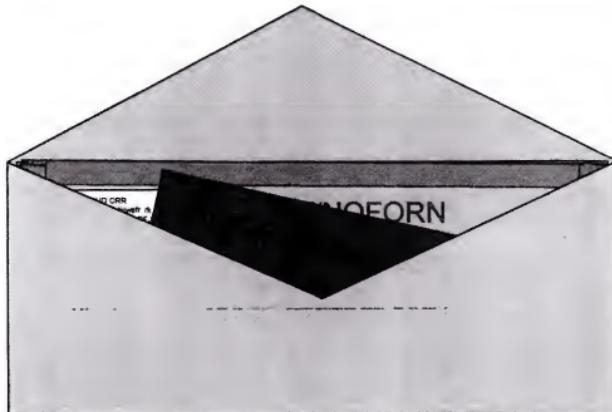
page 95, para 8-10b



- Address of sender
- Address of receiving activity - May have Attention line with person's name
- Highest Classification of the contents
- Special Marking such as:
 - “RESRICTED DATA”
 - “NATO”
- Special Instructions- if needed



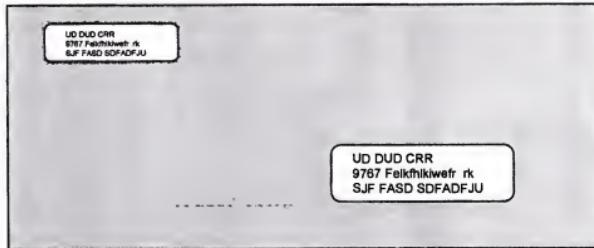
STEP SEVEN



- Insert a “return” Receipt & Place into the 2nd Envelope (Outer)



STEP EIGHT



- **Address information**

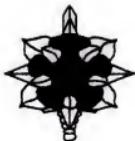


Address/Marking Information for Outer envelope

page 95, para 8-10



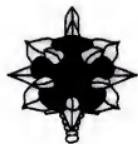
- Address of sender
- Address of receiving activity such as:
 - Official Government agency/Unit
 - Cleared DOD contractor facility
- May use Office codes or phrases such as
 - “Attention: Research Department”
- May NOT be addressed to an Individual
- Will not bear Classification markings,
special markings or any other unusual marks
that may draw attention



STEP NINE



- Place in Briefcase and Lock Briefcase
- Take to the U.S. Post Office
 - Send Registered Mail
- Wait for Classified Document receipt (DA Form 3964) from receiving agency acknowledging receipt of documents.



Student Check



What classification level can be sent registered mail?

Secret and Below



Methods of Destruction

page 18, para 3-15

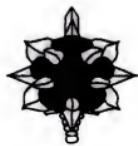


- **Burning** Preferred method for documents and overlays
- Crosscut Shredding
- Wet Pulping
- Pulverizing



When Destroying CD's, scratch the surface with a key or nail, then break the CD in to several small pieces or burn.

Complete the DA Form3964 (certificate of destruction)



QUESTIONS???





Enabling Learning Objective C



ACTION: Provide Information About Operations Security to the World Wide Web

CONDITIONS: Given Classroom Instruction

STANDARD: Provided a list of aspects related to Operations Security violations on the World Wide Web



ELO Agenda



ELO C: Apply Operations Security to the World Wide Web

- What is Operations Security (OPSEC)
- Different types of critical information
- How to prevent disclosure of critical information



OPSEC



The enemy will attempt to discover how and when we are conducting operations, knowing this, we must protect our activities from detection.

We do this by:

- Identifying - Critical Information**
- Analyzing - Threat**

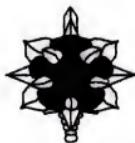


Critical Information



- Photos
- Installation maps with highlights of designated points of interest (sleep/work, CDR, dining facility, etc)
- Security Operating Procedures (SOPs)
- Tactics, Techniques and Procedures (TTPs)
- Unit Capabilities and Intent
- Unit morale
- Personal/Family Information

Sensitive Information

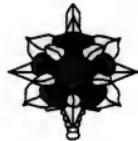


Prevent Disclosure



- DON'T DISCUSS OPERATIONAL ACTIVITIES ON THE WEB or E-mail
- Ensure information posted has no significant value to the adversary
- Consider the audience when you're posting to a blog, personal web page or Email
- Always assume the adversary is reading your material
- Work with your OPSEC Officer – follow policies and procedures!

Remember it is called the World Wide Web for a reason



Student Checks



What is Critical Information?

It is anything that helps the enemy obtain an advantage over us.

How can we prevent disclosure of Critical Information?

**Follow OPSEC
Policies & Procedures**



Summary



ELO A: Annotate Classification Markings to a Document- Answer 12 of 15 questions correctly



ELO B: Apply Procedures for Protecting Classified Information- Answer 12 of 15 questions correctly



ELO C: Provide information about Operation Security and the World Wide Web - Not tested



QUESTIONS???



Intelligence Analyst Course

Course/Version: 243-35F10 / 001

Delivery Group/Phase: A / 0

Status: Commandant Approved as of 2008-10-02

TABLE OF CONTENTS

	<u>PAGE</u>
Lesson 1 Section I Administrative Data	4
Section II Introduction.....	7
Terminal Learning Objective - Identify 35F10 Course Administrative and Academic policies	7
Section III Presentation	9
Section IV Summary.....	10
Section V Student Evaluation.....	11
Lesson 2 Section I Administrative Data	12
Section II Introduction.....	15
Terminal Learning Objective - Identify principles of protecting classified information, material and media.....	15
Section III Presentation	17
Section IV Summary.....	53
Section V Student Evaluation.....	54
Lesson 3 Section I Administrative Data	55
Section II Introduction.....	58
Terminal Learning Objective - Present Intelligence Findings.....	58
Section III Presentation	65
Section IV Summary.....	461
Section V Student Evaluation.....	463
Lesson 4 Section I Administrative Data	464
Section II Introduction.....	468
Terminal Learning Objective - Perform Map Analysis and Construct Proper Military Symbology	468
Section III Presentation	470
Section IV Summary.....	577
Section V Student Evaluation.....	578
Lesson 5 Section I Administrative Data	579
Section II Introduction.....	582
Terminal Learning Objective - Define the Operational Environment and Identify U.S. Warfighting Doctrine	592
Section III Presentation	606
Section IV Summary.....	617
Section V Student Evaluation.....	618
Lesson 6 Section I Administrative Data	619
Section II Introduction.....	622

	Terminal Learning Objective - Describe the Battlefield Effects	632
	Section III Presentation	645
	Section IV Summary.....	657
	Section V Student Evaluation	658
Lesson 7	Section I Administrative Data	659
	Section II Introduction.....	662
	Terminal Learning Objective - Evaluate the Threat.....	662
	Section III Presentation	664
	Section IV Summary.....	670
	Section V Student Evaluation	671
Lesson 8	Section I Administrative Data	672
	Section II Introduction.....	675
	Terminal Learning Objective - Determine Threat Courses of Action (COA)	675
	Section III Presentation	677
	Section IV Summary.....	692
	Section V Student Evaluation.....	693
Lesson 9	Section I Administrative Data	694
	Section II Introduction.....	697
	Terminal Learning Objective - Draft an ISR Plan	697
	Section III Presentation	698
	Section IV Summary.....	702
	Section V Student Evaluation.....	703
Lesson 10	Section I Administrative Data	704
	Section II Introduction.....	708
	Terminal Learning Objective - Conduct Targeting in Phase III and Phase IV Operations	708
	Section III Presentation	710
	Section IV Summary.....	791
	Section V Student Evaluation.....	792
Lesson 11	Section I Administrative Data	793
	Section II Introduction.....	796
	Terminal Learning Objective - Conduct Intelligence Analysis	796
	Section III Presentation	797
	Section IV Summary.....	807
	Section V Student Evaluation.....	808
Lesson 12	Section I Administrative Data	809
	Section II Introduction.....	812
	Terminal Learning Objective - Produce the products for the Mission Analysis	812
	Section III Presentation	814
	Section IV Summary.....	821
	Section V Student Evaluation.....	822
Lesson 13	Section I Administrative Data	823

Section II	Introduction.....	827
	Terminal Learning Objective - Conduct Intelligence Analysis	827
Section III	Presentation	829
Section IV	Summary.....	842
Section V	Student Evaluation.....	843
Lesson 14	Section I Administrative Data	844
	Section II Introduction.....	848
	Terminal Learning Objective - Qualify Soldiers on Core Warrior Tasks and Battle Drills	848
	Section III Presentation	849
	Section IV Summary.....	851
	Section V Student Evaluation.....	852
Appendix A	- Viewgraph Masters (N/A) A -	1
Appendix B	- Test(s) and Test Solution(s) (N/A) B -.....	1
Appendix C	- Practical Exercises and Solutions (N/A) C -	1
Appendix D	- Student Handouts (N/A) D -	1

Prosecution Exhibit 55

1 page
classified
"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order
dated 20 August 2013
stored in the classified
supplement to the original
Record of Trial

Prosecution Exhibit 56

1 page
classified
"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order
dated 20 August 2013
stored in the classified
supplement to the original
Record of Trial

Prosecution Exhibit 58

2 pages
classified

"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order
dated 20 August 2013
stored in the classified
supplement to the original
Record of Trial

AN AGREEMENT BETWEEN

BRADLEY EDWARD MANNING

AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, "the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.
10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.FOR OFFICIAL USE ONLY
Law Enforcement SensitiveSTANDARD FORM 312 (REV. 1-91)
Prescribed by GSA/ISO
32 CFR 2003, E.O. 12356

USAPPC V2.00

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing offices has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE 	DATE 07 APR 08	SOCIAL SECURITY NUMBER (See Notice below) 445 98 9504
--	-------------------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)
(Type or Print)

Company: D CO
Battalion: 305TH MI BN
Fort Huachuca, Arizona 85613

Attestation completed on: 07 APR 08

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE Elisa K. Rubin	DATE 07 APR 2008	SIGNATURE Elisa K. Rubin	DATE 07 APR 2008
NAME AND ADDRESS (Type or print) Commander, USAIC&FH ATTN: ATZS-GI-E Building # 22320, Augur Avenue Fort Huachuca, AZ 85613-6000		NAME AND ADDRESS (Type or print) Commander, USAIC&FH ATTN: ATZS-GI-E Building # 22320, Augur Avenue Fort Huachuca, AZ 85613-6000	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to (1) certify that you have access to the information indicated above or (2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

STANDARD FORM 312 BACK (REV. 1-91)

USAPPC V2.00

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

MANNING Bradley
(Name of individual - Printed or typed)

AND THE UNITED STATES

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 14(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, "952 and 1924, Title 18, United States Code," the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable

STANDARD FORM 312 (REV 1-00)
Prescribed by NAVFAC/DO
32 CFR 2003, E.O. 12858
AFP PZ v1.00

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7.211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identifies Protection Act of 1982 (60 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its Implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
	17 SEP 08	445-98-9504
ORGANIZATION (IF CONTRACTOR, LICENSEE, OR AGENT, PROVIDE NAME, ADDRESS, AND, IF PUBL., FEDERAL SUPPLY CODE NUMBER) (Type or Print)		

Manning, Bradley, Edward
10100 N. Riva Ridge LP
FT Drum, NY 13602

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.
SIGNATURE 	SIGNATURE
NAME AND ADDRESS (Type or print) Belonek, Kyle J 10100 N. Riva Ridge Loop FT. Drum, NY 13601	NAME AND ADDRESS (Type or print) Stark, Loren J 10100 N. Riva Ridge Loop FT. Drum, NY 13601

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have retained all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information; and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to: 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT

STANDARD FORM 312 BACK (REV. 1-00)
AFDPFv1.00

Prosecution Exhibit 61

2 CDs

classified

"SECRET"

ordered sealed for Reason 2
Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Prosecution Exhibit 62

2 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Views of ACIC Product RB08-0617.asp

Record Key	IP Address	Visit Date	Record Key	IP Address	Visit Date
Views of ACIC Product RB08-0617.asp					
Record Key	IP Address	Visit Date	Record Key	IP Address	Visit Date
734639	199.123.68.193	3/18/08 9:25 AM	735324	128.80.137.173	3/18/08 8:41 PM
734648	22.21.192.158	3/18/08 9:28 AM	988665	128.80.137.173	5/30/08 7:41 PM
734651	22.4.28.24	3/18/08 9:28 AM	737131	128.80.137.83	3/20/08 7:09 PM
734667	22.21.192.159	3/18/08 9:39 AM	1034511	128.80.15.100	6/2/08 7:54 PM
734669	22.21.14.179	3/18/08 9:40 AM	1029749	128.80.15.76	6/2/08 2:39 PM
734673	148.124.231.32	3/18/08 9:43 AM	2557569	128.80.150.120	12/19/08 11:20 PM
734691	22.21.14.160	3/18/08 9:56 AM	737839	128.80.153.111	3/21/08 8:07 PM
734692	164.222.90.99	3/18/08 9:58 AM	738271	128.80.240.63	3/24/08 2:46 AM
734696	199.123.68.193	3/18/08 10:03 AM	736079	130.90.23.204	3/19/08 1:22 PM
734700	22.21.9.95	3/18/08 10:04 AM	3442471	131.21.139.173	10/23/09 6:19 AM
734708	207.85.61.114	3/18/08 10:05 AM	3442971	131.21.139.173	10/23/09 6:31 AM
734709	164.222.90.99	3/18/08 10:05 AM	737225	131.240.17.34	3/21/08 6:09 AM
734710	22.15.141.48	3/18/08 10:05 AM	737442	131.240.17.34	3/21/08 9:36 AM
734711	22.13.44.234	3/18/08 10:05 AM	2795854	131.240.53.121	3/16/09 7:01 AM
734759	205.14.113.91	3/18/08 10:22 AM	777461	131.240.53.95	5/3/08 6:32 PM
734770	21.245.1.4	3/18/08 10:27 AM	1955211	132.143.11.57	7/2/08 1:18 PM
734771	21.245.1.4	3/18/08 10:27 AM	735146	132.143.125.137	3/18/08 2:40 PM
734773	22.21.192.156	3/18/08 10:28 AM	737803	132.143.125.21	3/21/08 4:22 PM
734785	204.36.183.206	3/18/08 10:32 AM	734918	132.143.200.154	3/18/08 12:27 PM
734788	22.21.14.171	3/18/08 10:33 AM	734988	132.143.200.154	3/18/08 1:04 PM
734793	207.84.120.78	3/18/08 10:35 AM	2551140	132.143.59.182	12/17/08 9:12 AM
734804	148.124.231.32	3/18/08 10:41 AM	2551243	132.143.59.182	12/17/08 10:02 AM
734820	147.254.122.140	3/18/08 10:57 AM	737651	132.143.9.35	3/21/08 2:03 PM
734826	143.175.195.27	3/18/08 11:01 AM	736123	137.13.1.126	3/19/08 1:38 PM
734842	204.20.165.38	3/18/08 11:12 AM	3858179	137.13.136.218	3/16/10 9:18 AM
734846	22.4.151.134	3/18/08 11:15 AM	736792	137.13.24.220	3/20/08 12:01 PM
734849	204.20.143.46	3/18/08 11:28 AM	735504	138.165.27.1	3/19/08 7:23 AM
734850	22.21.14.171	3/18/08 11:28 AM	735058	138.17.47.252	3/18/08 1:35 PM
734851	207.85.68.123	3/18/08 11:28 AM	1952310	138.45.41.10	7/2/08 9:58 AM
734857	157.214.254.158	3/18/08 11:30 AM	2082281	138.45.41.7	7/10/08 11:02 AM
734860	206.36.90.135	3/18/08 11:31 AM	1953626	138.45.43.6	7/2/08 11:31 AM
734861	157.202.36.134	3/18/08 11:31 AM	2333393	138.45.43.7	9/8/08 1:37 PM

P2

PROSECUTION EXHIBIT 43 for identification
 PAGE OFFERED: _____ PAGE ADMITTED: _____
 PAGE OF PAGES

Views of ACIC Product RB08-0617.asp

Record Key	IP Address	Visit Date
734868	204.20.81.51	3/18/08 11:39 AM
734869	22.21.14.171	3/18/08 11:40 AM
734882	157.224.197.144	3/18/08 11:53 AM
734884	22.20.98.171	3/18/08 11:57 AM
734886	22.21.14.170	3/18/08 11:58 AM
734897	207.85.134.181	3/18/08 12:13 PM
734903	148.124.19.196	3/18/08 12:18 PM
734905	147.254.27.40	3/18/08 12:19 PM
734911	22.2.53.66	3/18/08 12:22 PM
734912	206.36.111.195	3/18/08 12:22 PM
734918	132.143.200.154	3/18/08 12:27 PM
734919	22.21.14.185	3/18/08 12:29 PM
734921	199.123.69.181	3/18/08 12:29 PM
734933	22.4.151.114	3/18/08 12:33 PM
734934	22.21.14.168	3/18/08 12:34 PM
734964	22.20.98.15	3/18/08 12:46 PM
734966	22.2.183.1	3/18/08 12:47 PM
734975	204.21.231.171	3/18/08 12:52 PM
734983	139.36.186.14	3/18/08 12:58 PM
734986	21.245.1.4	3/18/08 1:02 PM
734988	132.143.200.154	3/18/08 1:04 PM
735001	148.124.95.30	3/18/08 1:11 PM
735009	148.124.4.42	3/18/08 1:14 PM
735013	199.31.33.154	3/18/08 1:18 PM
735015	148.124.193.41	3/18/08 1:18 PM
735016	148.124.193.41	3/18/08 1:18 PM
735020	148.124.193.41	3/18/08 1:19 PM
735021	148.124.193.41	3/18/08 1:19 PM
735043	148.124.186.40	3/18/08 1:30 PM
735044	22.21.14.184	3/18/08 1:30 PM
735046	22.5.185.19	3/18/08 1:30 PM
735058	138.17.47.252	3/18/08 1:35 PM
735066	207.84.120.70	3/18/08 1:37 PM
735077	22.45.248.192	3/18/08 1:44 PM

Record Key	IP Address	Visit Date
2058058	138.45.45.25	7/7/08 1:35 PM
1635369	139.32.17.34	6/20/08 4:59 AM
1635448	139.32.17.34	6/20/08 5:04 AM
734983	139.36.186.14	3/18/08 12:58 PM
735366	141.220.71.26	3/19/08 2:56 AM
736364	141.220.71.26	3/20/08 5:04 AM
2407341	141.220.71.26	10/9/08 6:05 AM
1851954	141.220.71.27	6/27/08 10:35 AM
1906032	141.220.71.27	6/30/08 6:03 AM
1925023	141.220.71.27	7/1/08 3:27 AM
1925157	141.220.71.27	7/1/08 3:35 AM
735106	143.175.111.53	3/18/08 2:13 PM
760027	143.175.111.53	4/10/08 12:27 PM
734826	143.175.195.27	3/18/08 11:01 AM
735805	143.57.168.31	3/19/08 9:24 AM
742755	143.57.168.31	3/27/08 8:07 AM
737412	143.57.168.34	3/21/08 9:17 AM
738336	143.57.168.35	3/24/08 6:25 AM
745466	143.75.50.241	3/30/08 11:34 PM
745467	143.75.50.241	3/30/08 11:34 PM
745468	143.75.50.241	3/30/08 11:34 PM
755219	143.75.50.241	4/6/08 7:07 PM
744023	144.19.37.37	3/28/08 2:37 PM
2663482	146.98.129.172	2/3/09 3:13 AM
2715530	146.98.194.50	2/25/09 3:38 AM
2663463	146.98.204.43	2/3/09 2:51 AM
741914	147.254.107.74	3/26/08 9:47 AM
734820	147.254.122.140	3/18/08 10:57 AM
746043	147.254.140.58	3/31/08 12:09 PM
750439	147.254.140.58	4/3/08 9:29 AM
3285341	147.254.166.61	7/24/09 9:46 AM
3285517	147.254.166.61	7/24/09 1:27 PM
3285538	147.254.166.61	7/24/09 1:52 PM
737060	147.254.171.184	3/20/08 3:09 PM

INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

USE OF FORM - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

COPIES - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

ARRANGEMENT - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.
2. Judge advocate's review pursuant to Article 64(a), if any.
3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.
4. Briefs of counsel submitted after trial, if any (Article 38(c)).
5. DD Form 494, "Court-Martial Data Sheet."
6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.
7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).
9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).
10. Congressional inquiries and replies, if any.
11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.
12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.
13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).
14. Records of former trials.
15. Record of trial in the following order:
 - a. Errata sheet, if any.
 - b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.
 - c. Record of proceedings in court, including Article 39(a) sessions, if any.
 - d. Authentication sheet, followed by certificate of correction, if any.
 - e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.
 - f. Exhibits admitted in evidence.
 - g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.
 - h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.